Departamento de Informática

PROYECTO FIN DE CARRERA

"Elaboración de planes de contingencia. Caso práctico: empresa de elevadores"

INGENIERIA INFORMÁTICA

Autor: OSCAR GARCÍA MUGA

Tutor: MIGUEL ÁNGEL RAMOS

Leganés, Junio de 2015.

Título: Elaboración de planes de contingencia. Caso práctico: empresa de elevadores.

Autor: OSCAR GARCÍA MUGA

Director: MIGUEL ÁNGEL RAMOS

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día _____ de _____ de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de _____

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Me gustaría expresar mi agradecimiento a mi profesor Miguel Ángel Ramos. Sin su ayuda, su experiencia, y sobre todo su paciencia, este proyecto no habría sido posible. He contado en todo momento con su apoyo, y en los momentos más difíciles, siempre ha tenido palabras de aliento. Muchas gracias, Miguel Ángel.

También quiero dar las gracias a mi madre y a mi padre, porque siempre me han apoyado en todo lo que he hecho y me han enseñado a confiar en mí mismo. Eso es fundamental para que las cosas salgan bien, para ser capaz de acabar lo se empieza. Me compraron mi primer ordenador cuando tenía 11 años y decidí que quería ser informático. Y durante los momentos duros de la carrera, esas asignaturas imposibles de aprobar, siempre sentí su apoyo.

También a mi abuela Marina, con la que tanto comparto. Que siempre ponía una vela cuando tenía un examen, y que seguro que ha puesto unas cuantas estos meses. Gracias abuela, eres la mejor.

A mis compañeros de carrera y sin embargo amigos, Víctor, Ángel y David. Durante estos años siempre me han estado preguntando: “bueno, y como ¿llevas el proyecto? Y sentir esa presión me ha ayudado a ponerme a ello, a no dejarlo. Gracias a los tres.

Y por supuesto a Bea, mi compañera, la persona con la que comparto mi vida. Que me ha visto durante estos meses sentado en el ordenador, sin moverme apenas, preguntándose qué clase de friki tengo en casa. Pero que me ha dado ánimos para terminarlo y ha escuchado mis cosas de informático con mucha paciencia.

Resumen

El actual mundo empresarial es muy complejo, globalizado y competitivo. Ello hace que los servicios que las empresas proporcionan a sus clientes también lo sean. Cada vez los servicios empresariales se demandan en más ubicaciones físicas y en unos horarios cada vez más amplios. Las compañías que quieran ser líderes en su sector, no pueden negar este hecho. Además, las implicaciones legales y mandatos regulatorios que se deben cumplir (sobre todo en lo relativo a seguridad y salud laboral) son cada vez más exigentes, y su incumplimiento puede provocar grandes pérdidas económicas, materiales o peor aún, de vidas humanas.

Por todo ello, es imprescindible la elaboración y mantenimiento de planes de contingencia para los servicios, especialmente para los más críticos y/o que más implicaciones legales puedan tener. De esta forma, las compañías estarán preparadas para atender cualquier contingencia que pueda surgir, y garantizar en cualquier circunstancia el servicio a sus clientes.

Para este propósito, las normas UNE 71599:2010 e ISO 22301 incluyen todas las recomendaciones a seguir para la elaboración de estos planes de contingencia. Estos planes bien pueden ser globales para toda la empresa, pero en función de su tamaño, podría ser interesante realizarlos por áreas, departamentos o procesos empresariales.

En el caso que nos ocupa, se ha desarrollado el plan de contingencia para un centro de control de una empresa de elevación. Se trata del departamento responsable de la atención a incidencias y rescates en aparatos elevadores, y por tanto, es estratégico para la empresa. Desde dicho departamento, se coordinan todas las operaciones de rescate de personas atrapadas en ascensores, y las incidencias que puedan dejar dichos aparatos y escaleras mecánicas fuera de servicio.

Para la empresa es fundamental que dicho departamento pueda ofrecer su servicio veinticuatro horas al día, trescientos sesenta y cinco días al año. De lo contrario podría tener problemas legales (en función de la comunidad autónoma hay unos tiempos máximos para acudir al rescate de personas atrapadas en un ascensor) y económicos (daño a la imagen de marca, perdidas de contratos, pago de penalizaciones por incumplimiento de nivel de servicio,…)

Palabras clave: plan contingencia, continuidad negocio, elevación, centro de control,

Abstract

The current business world is very competitive, globalized and complex. This means that the company services to customers are complex, competitive and globalized too. More every day, those services are demanded around the whole world and expanding the public opening times. The companies, who want to be leaders, should improve on it. Besides the fact that legal requirements and rules that the companies must obey (especially regarding safety and occupational health) are more demanding every day, and the unfulfilment would bring less economic losses, material losses, or in the worst case scenario, heavy casualties.

Because of this, it's mandatory to work in build and maintain contingency planning for the services, primarily the more critical and/or those who more legal requirements have. At this way, the companies will be ready to solve any eventuality that would happen, and get the customer services running.

In order to reach this goal, the companies can follow ISO 22301 and UNE 71599:201. This both standards give the recommendations to develop this contingency planning. This plans would be for the whole company, but if the company is very big, it should be interesting work out in areas, company process or departments.

In the current project, we are develop the contingency plan for an elevator company service center. This department is responsible for customers call center and rescues on the elevators. Because of this, it's a strategic department for the company. From this department, are coordinated all rescue operations for people trapped in an elevator, and any contingency that would be the elevator or escalator out of service.

For the company is essential that this department be able to give the services twenty four hours per day, three hundred and sixty five days per year. Otherwise, the company would have legal problems (depending of the state, there are different times to rescue people trapped in an elevator) and economic loss (lose contracts, pay penalties for break the service level agreement, damage the company reputation…)

.

Keywords: contingency planning, business continuity, elevator, service center

Índice

Indicé de figuras

Índice de tablas

Introducción.

1.1 Ámbito General del Problema

En el mundo empresarial cada vez son más los servicios críticos que requieren estar operativos 24 horas al día, 365 días al año. Hace no tantos años, la mayoría de las empresas paralizaban su actividad durante el mes de agosto y en muy pocos casos se planteaban mantener su actividad los fines de semana o fuera de la jornada habitual del país en el que desempeñaban su actividad. Pero las necesidades de los mercados, tan globales y tan cambiantes, han modificado esta tendencia.

En la actualidad, la mayoría de las empresas continúan trabajando en agosto, con menor intensidad que el resto de meses, pero trabajando. Y los fines de semana, aunque la actividad no sea la misma, en muchos casos hay que dar servicio a clientes, lo que implica que bien presencialmente, bien en forma de guardias o turnos, la actividad no se frena. De esta forma, nos podemos encontrar con grandes corporaciones de ámbito mundial, que tienen dividida su actividad por regiones físicas, afinidad cultural o necesidades del propio negocio.

Por ejemplo, se da el caso de empresas con una unidad de negocio que incluye el sur de Europa, el continente africano y Oriente Medio. En este caso, al incluirse países con distintas zonas horarias y diferentes costumbres culturales, el soporte del tipo que sea tiene que abarcar toda la semana puesto que el fin de semana por ejemplo, no es los mismos días de la semana en Qatar que en Portugal. El domingo festivo en Portugal, no lo es en Qatar. Si se quiere dar servicio del tipo que sea (informático, legislativo, financiero, rrhh,..) desde Portugal a Qatar o viceversa, hay que tener estos detalles en cuenta.

A continuación se muestra una tabla del Informe anual mundial de Symantec sobre la complejidad y criticidad de los servicios. Se trata de un informe que la compañía genera a partir de encuestas que realiza a 2432 empresas de 32 países. Aparece en primer lugar de los factores que crean complejidad con un porcentaje de un 65% el incremento de las aplicaciones críticas para el negocio. En segundo lugar aparece el crecimiento de los datos, sobre todo los de las aplicaciones críticas y a continuación la movilidad y la virtualización.

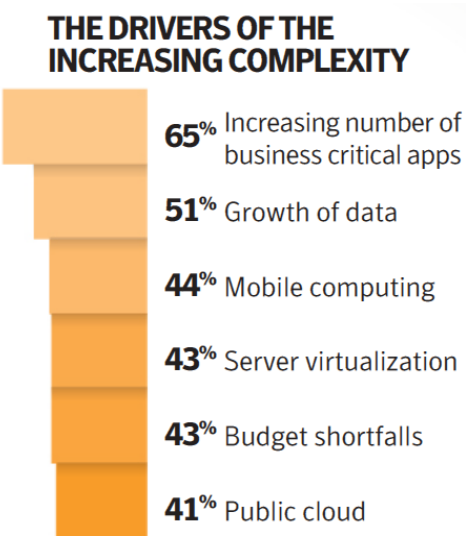


Figura 1

Esta criticidad de servicios no debe ser menospreciada. En la figura 2, también obtenida del informe de Symantec se puede apreciar que 16 fallos en los sistemas de una compañía media de nivel mundial pueden suponer unas pérdidas de 5,1 millones de dólares, y que la mayor parte de ellos son provocados por fallos en el sistema, concretamente el 68.75%. En cambio los errores humanos solo representan un 25% y los desastres naturales poco más de un 6%. Por tanto, y dado que la mayoría de los tiempos de caída del sistema dependen de fallos en el mismo, parece buena idea tener un sistema de respaldo que nos pueda proteger de ellos.

En la figura 3 se pueden ver las consecuencias de los fallos en sistemas críticos. Casi la mitad de ellos suponen un incremento de los costes para la compañía y casi un 35% suponen problemas de seguridad y que el sistema deje de estar operativo.

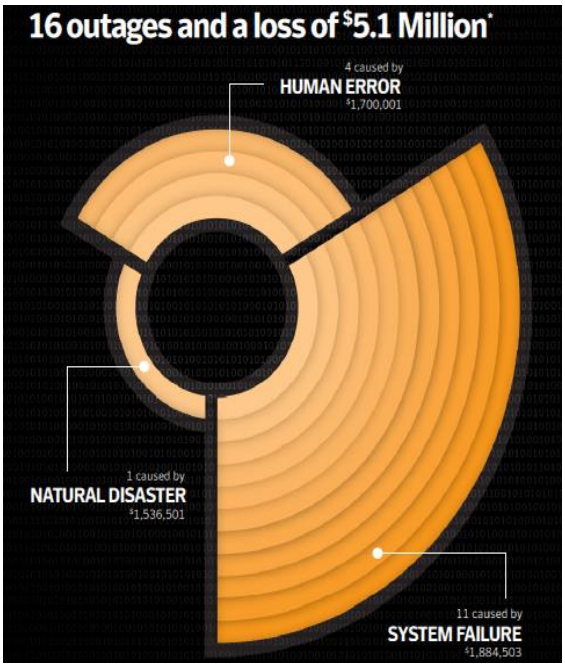


Figura 2

Figura 3

Es por eso que en muchos de los casos es la propia empresa la que decide que un servicio es crítico con lo que el plan de contingencia de dicho servicio puede proporcionarle una importante ventaja competitiva. Por ejemplo, con el objetivo de reducir costes, una empresa puede decidir centralizar su software de operaciones en uno de los países de su unidad de negocio. Desde por ejemplo España, se da el servicio a toda Europa y América del Sur. De esta forma la empresa reduce costes, puesto que no necesita tener personal en cada uno de los países, no necesita tanto hardware y se comparten los gastos entre las filiales de los diferentes países. Pero en ese caso el servicio es crítico y dada la diferencia horaria entre España y los países de Sudamérica el servicio debe darse prácticamente 24 horas al día.

En otras ocasiones es la ley la que obliga a la empresa a dar un determinado servicio en estas condiciones, so pena de implicaciones jurídicas, ya sean mercantiles, administrativas o penales. El caso que nos ocupa pertenece a este último. Una empresa que basa su negocio en el mantenimiento de aparatos elevadores, debe proporcionar un servicio de rescate de 24 horas, 365 días al año. Cuando se produce una avería en el aparato y una persona o varias quedan atrapadas dentro de la cabina, la empresa responsable del mantenimiento tiene el deber de proceder al rescate y liberarlas a la mayor brevedad posible. Para ello, dicha empresa debe tener un complejo sistema informático y de telecomunicaciones, con el fin de recibir la llamada de emergencia, identificar el aparato (modelo, lugar de la instalación y demás detalles) y el tipo de incidencia que ha sufrido, para en el menor tiempo posible ponerse en contacto con un técnico, y que acuda a realizar el servicio correspondiente.

Algunas de las ventajas que obtiene la compañía desarrollando e implementando un plan de contingencia pueden verse en la siguiente figura:

Figura 4

Por otra parte, el sistema es mucho más completo y fiable si funciona de un modo proactivo. Es decir, si se tiene la información actualizada del parque de elevadores y escaleras mecánicas, y si hay una telealarma automática. Entendemos por telealarma un sistema en el que un ascensor se comunica con la central de mantenimientos para indicarle el estado en que se encuentra, el tiempo que falta para la siguiente revisión y algunos datos técnicos. Esto puede hacerse bien por una llamada de teléfono, bien por sms o bien mediante un correo electrónico. De esta forma, la empresa dispone de la información con antelación y la reparación de una avería de pequeño calado a tiempo, puede prevenir una mayor. Además de que la imagen comercial de la empresa, muy importante en un mundo globalizado donde la información circula a gran velocidad, no se ve afectada si la pequeña avería se soluciona de forma interna sin prejuicios para el cliente.

Todo ello requiere la implantación de un sistema que sea capaz de automatizar todo este proceso, cubrir los requisitos de los usuarios y estar operativo las 24 horas del día, 365 días al año. Y la mejor forma de garantizar esta alta disponibilidad es disponer de otro centro de respaldo. De esta forma, cuando el problema sea de menor envergadura, se podrá resolver dentro del centro principal. Y en el caso de que la contingencia sea mayor e inutilice el centro primario, se pueda poner operativo en poco tiempo un centro alternativo desde el que se ofrezca el servicio. Una contingencia severa podría ser el incendio, una inundación o desastre natural que inutilice el centro principal durante un periodo largo de tiempo.

Los periodos de tiempo de recuperación de cada uno de los servicios serán definidos por el o los responsables de cada uno de los servicios. De igual manera deberán ser ellos los que definan la degradación máxima que puede soportar cada uno de los sistemas, para poder continuar operando con relativa normalidad.

1.2 Problema en sí

Una vez que la empresa de elevadores tiene implementado dicho servicio, y tal y como se ha detallado en el apartado anterior, surge la necesidad de la alta disponibilidad del mismo. La empresa tiene que ser capaz de ofrecer dicho servicio independientemente de las contingencias que puedan surgir:

- Averías parciales → el sistema está operativo al completo. Pero alguno de los subsistemas que lo forman tiene alguna pequeña incidencia, que aunque no le impide operar, dificulta su funcionamiento. Ejemplos de este tipo de averías puede ser el que no esté operativo el servicio de identificación de llamada. No impide que el sistema ni ninguno de los subsistemas tenga que detenerse, pero dificulta la labor del operador que tiene que localizar

manualmente los datos del elevador sobre el que se abre la incidencia.

- Averías parciales severas→ el sistema continuo funcionado, pero alguno de los subsistemas que lo forman no está operativo: avería de los sistemas informáticos, avería de los sistemas de telecomunicaciones. Ejemplos de este tipo de averías podrían ser que se estropea la centralita, que haya una avería en los equipos del proveedor de comunicaciones o hay alguna avería en los servidores donde corre la aplicación que utilizan los operadores que recepcionan llamadas.

- Averías totales → ninguno de los diferentes subsistemas están operativos, por lo que la empresa no puede ofrecer el servicio. Este es el caso de un incendio en la ubicación física donde se encuentran los equipos que proporcionan el servicio, una inundación o cualquier otra contingencia que inutilice totalmente el sistema.

Evidentemente cada uno de estos tipos de avería tendrá un tratamiento distinto, en función de su severidad, en función del día y la hora en que se produzca. No es lo mismo que la avería se produzca en horario laborable, cuando las delegaciones de dicha empresa se encuentran operativas y pueden dar el servicio, que si se producen un sábado a las 4 de la mañana, cuando no se puede proporcionar el servicio desde otra ubicación.

Por ello será necesario realizar una completa y detallada definición de los servicios y de los tiempos máximos de restauración de cada uno de ellos. Para ello se contará con el personal del departamento CC24h que deberá indicar cuál es el tiempo máximo asumible que se puede mantener uno de los servicios no operativo. En función de esta definición de tiempos, el sistema podrá variar, tanto en su diseño como en su coste. Cuanto menor sea el tiempo tolerable de parada de un servicio por su criticidad, mayor será el coste económico que tendrá. Dicha criticidad obligará a disponer de mayores recursos, tanto materiales como humanos.

Por ejemplo, supongamos que uno de los servicios identificados como críticos es el sistema de gestión de averías, donde los operadores van introduciendo los datos de la avería del ascensor. Para ello necesitan tener disponibles las líneas de teléfonos por las que se reciben las llamadas, los puestos con el software que conecta como cliente, un buzón de correo electrónico y el clúster donde se encuentra la aplicación.

Si se decide que no se puede dar el servicio del departamento durante más de 2 horas sin este servicio, el coste del procedimiento sería bastante elevado. Se necesitaría tener disponible otro servidor con los

datos actualizados (lo que implica sincronización de datos prácticamente en línea), otro servidor de correo electrónico desde el que se pudiera utilizar el buzón, recursos humanos para realizar la configuración del cliente, recursos humanos para configurar el correo electrónico y recursos humanos para gestionar los cambios de telecomunicaciones con el operador.

En cambio, si una de las aplicaciones que realiza el teleservicio se considera que no es crítica y que se puede prescindir de ella durante 2 días, el coste resulta mucho menor. En este caso se podría restaurar una imagen del mismo en otra máquina y no se requerirían recursos humanos adicionales, puesto que se podría realizar en jornada laboral, ahorrándose bastante dinero en horas extras y disponibilidad del personal.

La mejor opción para garantizar el funcionamiento de este sistema consistirá en elaborar un completo plan de contingencias para dar respuesta a las posibles incidencias en el sistema. Dicho plan incluirá la implementación y mantenimiento de un centro de respaldo desde el que se dará el servicio en caso de desastre en el centro principal. Para la puesta en marcha del centro de respaldo hay dos estrategias básicas que son el outsourcing y el desarrollo de un centro propio.

Para corporaciones de tamaño pequeño o medio, el outsourcing puede ser una buena opción. Pero para el caso de compañías como la que nos ocupa, con un parque de más de 100.000 aparatos, más de 100 oficinas y más de 4000 empleados, se considera mejor opción disponer de un centro propio. De esta forma se puede garantizar la calidad del servicio disponiendo de los medios adecuados, puesto que en el caso de preferir un outsourcing, es complicado conseguir que se cumplan los ANS (Acuerdos de nivel de servicio), puesto que son muy susceptibles de interpretaciones.

De hecho, la tendencia actual dentro de IT es la de gestionar los sistemas core de negocio con recursos propios, como única forma de garantizar la calidad del servicio, la escalabilidad del sistema y la evolución del mismo. Actualmente ha aparecido en la prensa española, en concreto en la revista Cinco Días, el caso de la compañía Telefónica que tras numerosos fracasos en proyectos de outsourcing, ha decidido comenzar la internalización de las actividades.

1.3 Terminología

Durante el desarrollo de este proyecto se han utilizado las siguientes siglas y abreviaturas:

Teleservicio	Se trata del servicio mediante el cual el sistema recibe información de los aparatos. Incluye información de estado y de control.
Telealarma	Se trata de una alarma que se dispara cuando algún aparato sufre alguna incidencia.
Aparato	Se trata de los aparatos de los que la empresa realiza mantenimiento: ascensores y escaleras mecánicas.
CAT	Centro de atención telefónica, el sistema que recibe las llamadas con las averías y comunica con los técnicos para proceder a los rescates y/o reparaciones requeridas
Dielro	Aplicación comercial de telealarma
EAR	Aplicación de la empresa para las telealarmas
Rescate	Intervención de un técnico de ascensores cuando un usuario se ha quedado atrapado en un aparato
SAI	Sistema de alimentación ininterrumpida, mantiene los equipos informáticos en funcionamiento cuando hay cortes eléctricos breves.
Grupo electrógeno	Sistema de generación de energía mediante combustibles fósiles, utilizado cuando se producen cortes eléctricos prolongados
CC24H	Centro de control 24 horas, es el departamento responsable del servicio sobre el que se aborda el plan.
I+D	Departamento de investigación y desarrollo de la empresa
Soporte técnico 24x7x2	Soporte técnico de hardware y/o software 24 horas al día, 7 días a la semana con un tiempo de respuesta máximo de 2 horas
Soporte técnico 8x5x6	Igual que el anterior pero solo 8 horas al día (el horario laborable que se acuerde), 5 días a la semana (los días laborables) y con un tiempo de respuesta de 6 horas.
MPLS	Multiprotocol Label Switching. Tecnología de conmutación creada para proporcionar circuitos virtuales sobre redes IP. Ofrece mejoras sobre frame-relay, como la creación de VPN's e ingeniería de tráfico.
ADSL	Asymmetric Digital Subscriber Line. Tecnología de telecomunicaciones que permite establecer circuitos asimétricos, con distinta velocidad en cada sentido

	de la transmisión.
Raid 5	Configuración de discos a nivel hardware que permite tolerancia a fallos. Consiste en dividir los datos a nivel de bloques distribuyendo la información de paridad entre todos los discos del raid.
Centro de respaldo	Centro de proceso de datos específicamente diseñado para proporcionar servicio sustituyendo a otro CPD principal que ha sufrido alguna contingencia
Call Center	Centro de atención a usuarios
ANS o SLA	Acuerdo de nivel de servicio. Es el contrato que se firma entre proveedor y cliente sobre la calidad de los servicios ofrecidos (tiempos de respuesta, tiempos de resolución de incidencias,..).
Aplicaciones core de negocio	Se trata de la aplicación o aplicaciones desde las que se gestiona el negocio de la empresa: ERP, CRM
ERP	Enterprise resource planning, sistema empresarial cuya función consiste en la planificación de los recursos
CRM	Customer relationship management, sistema de gestión de las relaciones con los clients.
RFQ	Request for quotation, es un proceso empresarial por el cual se implica a los proveedores en la solicitud de una oferta, de forma que todos tengan que facilitar datos muy similares y se facilite la comparación de ofertas para su contratación.

Tabla 1

1.4 Enumeración de Capítulos

1. Descripción del sistema
    1.1. Centro de atención telefónica
    1.2. Sistemas de telealarmas.
        1.2.1.1. Teleservicio
        1.2.1.2. EAR
        1.2.1.3. Dielro.
        1.2.1.4. Escaleras
    1.3. Servicios afectados por el plan
    1.4. Tiempos máximos asumidos sin servicio
    1.5. Recogida y análisis de requisitos

2. Resolución de incidencias parciales

    2.1. Fallo en el suministro eléctrico
    2.2. Avería en telecomunicaciones
    2.3. Avería en servidores de CAT
    2.4. Avería en hardware de comunicaciones
    2.5. Avería en sistema de telealarma
    2.6. Avería en servicio de correo electrónico.
    2.7. Contingencia en el envío de mensajes a móviles
    2.8. Contingencia en servidores de datos
    2.9. Contingencia acceso corporativo a Internet

3. Recuperación del sistema completo
    3.1. Requisitos de la ubicación física
    3.2. Recursos humanos
    3.3. Infraestructura del centro de respaldo.
    3.4. Plan de actuación
    3.5. Varios

4. Evaluación del plan de contingencia
    4.1. Introducción
    4.2. Compatibilidad con la estrategia actual
    4.3. Viabilidad económica
    4.4. Simulacros
    4.5. Conclusiones.

2 Estado de la Cuestión

2.1 Descripción del sistema

En este punto se trata de describir a fondo el funcionamiento del sistema detallando al máximo los servicios, especialmente los más críticos. Será necesario ser lo más exhaustivo posible, para que ningún detalle quede fuera del plan. Es importante ser riguroso para que ningún pequeño detalle pueda dar al traste con nuestro objetivo. Por ejemplo sería inadmisible que tras organizar un completo plan de restauración del servicio, en el que se incluyeran los recursos materiales, las relaciones con proveedores, y los recursos humanos, el servidor elegido para realizar la restauración del sistema de averías tuviera un fallo en un dispositivo físico, en un disco duro por ejemplo, y quedara inutilizado. Se trata de detallar el sistema de tal manera que a la hora de la realización del diseño del plan se disponga de tanta información que sea complicado no estar preparado/a para cualquier contingencia. El objetivo es dejar al azar la menor parte posible de situaciones.

Puesto que el personal del departamento CC24H es el que conoce el sistema con mayor profundidad, se realizarán entrevistas a sus miembros, tratando de ver en qué forma y con qué medios trabajan. De esta forma, aparte de completar un completo plan de contingencias, se puede obtener una visión global del funcionamiento del servicio, e incluso ofrecer a dicho departamento mejoras en sus procesos. Dichas entrevistas pueden encontrarse en el anexo A de este proyecto.

2.1.1 Centro de atención telefónica

Este sistema es conocido por las siglas de su nombre, CAT. Se trata del sistema en el que los operadores recogen las llamadas de los clientes y registran las incidencias en los aparatos. Pueden ser llamadas de averías comunes y no urgentes (una puerta de un ascensor que no cierra bien o el led que indica el piso fundido) o averías criticas (rescate de una persona encerrada en un ascensor).

El proceso que se sigue es el siguiente

- El cliente observa una incidencia en algún aparato cuyo responsable de mantenimiento es la empresa y realiza una llamada al número de atención telefónica
- La llamada llega a una centralita y se pasa a un operador, en el caso de que haya alguno disponible. Si no hay ninguno disponible la llamada se mantiene en espera y se actualiza el led del CC24h que almacena dicha información
- Cuando la llamada pasa a un operador, se recibe en el display de su teléfono el número llamante. Mientras se atiende al cliente, se introduce el número de teléfono en el sistema.

- Si el número está asociado a algún aparato, el sistema muestra por pantalla toda la información del mismo. En ese mismo momento se dispone de la identificación del aparato, su ubicación física, el nombre del cliente y su historial de mantenimientos y averías.
  Esto sucede cuando el número de teléfono desde el que se realiza la llamada es el propio del aparato o bien es el teléfono de contacto de la persona que solicito la instalación del aparato.
- En el caso de que el número no estuviera asociado, el operador debe preguntar al cliente los datos necesarios para poder identificar el aparato. En el caso de que se trate de un elevador, se puede identificar bien por la dirección del mismo, bien por el número del aparato (cada ascensor tiene un ID único) que el cliente puede encontrar dentro de la cabina del mismo.
  En el caso de una escalera mecánica es necesario la ubicación física (en el caso de que sea una única escalera mecánica en la zona) o bien el identificador de la misma. En este caso suele ser más sencilla la identificación porque generalmente las escaleras mecánicas se encuentran en servicios públicos, centros comerciales o similares, y suele ser personal del mismo la que da parte de la avería.
- Una vez que el operador tiene todos los datos del aparato a su alcance, procede a registrar el detalle de la avería. En este punto es muy importante que la descripción de la incidencia sea lo más clara y concreta posible, para que el técnico que acudirá a repararlo tenga la mayor información posible. De esta forma, podrá acudir a la avería con el material necesario en el caso de que sea pertinente una sustitución, y con mayor o menor celeridad en función del tipo de incidencia. No es necesario señalar que no tiene la misa severidad una persona encerrada en un ascensor, que un ascensor inmovilizado vació o una puerta que no ajusta bien. De esta forma, y en función de la descripción de la avería que se pueda obtener del cliente, se asigna una severidad a la incidencia y se pone en la cola de averías pendientes para la asignación de técnico
- Una vez que el sistema asigna un técnico, esté recibe un correo electrónico en su dispositivo Blackberry. En dicho email aparece toda la información que el técnico requiere: identificador del aparato, dirección del mismo, modelo de aparato, pequeño resumen del historial del mismo (historial de averías, mantenimientos,….) y una descripción de la avería. Dicho correo genera además una tarea, que se coloca dentro de las tareas en función de la severidad de la misma. Por ejemplo, si se trata de un rescate de una o varias personas atrapadas en un aparato elevador se colocará en el primer lugar de la lista de tareas y si es un

ascensor que hace ruido al pasar entre la segunda y la tercera planta, se colocará al final de la misma.

- El técnico resuelve la incidencia o avería y envía un correo electrónico desde el dispositivo Blackberry o Android. En el indica todos los datos que ha recibido del departamento CC24H, junto con la descripción de los trabajos que ha realizado, las piezas utilizadas , los procedimientos que ha seguido y el tiempo que ha necesitado.
- El correo llega al buzón genérico del departamento CC24H y uno de los operadores registra en el sistema los datos recibidos del técnico y procede a dar por cerrada la incidencia. Todos los datos quedan almacenados en el historial del aparato.

2.1.2 Sistemas de telealarma.

Se trata de los sistemas para realizar el mantenimiento de los aparatos. Cada uno de los ascensores o escaleras mecánicas tienen instalado un sistema electrónico que registra las incidencias que se producen en el mismo, con fecha y hora. Cada 3 días envían a uno de los sistemas de teleservicio el estado en el que se encuentran, si tienen o no algún componente averiado e informan de las revisiones que deberán realizarse. Si algún aparato no envía en tres días un informe de su estado, un técnico debe ir a revisarlo físicamente, puesto que ello indica que ha habido algún problema, bien en el sistema electrónico de teleservicio, bien en el propio aparato.

Actualmente la empresa dispone de tres sistemas distintos de teleservicio para ascensores. El motivo es que inicialmente, cuando apareció la ley EN 81-28 en vigor en todos los países de la UE, que obliga a las empresas de mantenimiento de elevadores y escaleras mecánicas el mercado de sistemas de teleservicio apenas estaba desarrollado. En ese momento, la empresa que disponía de un departamento de I + D bastante importante decidió desarrollar su propio sistema y lo llamo teleservicio. Dicho sistema estuvo funcionando en solitario durante un año, pero se vio que no era viable mantenerlo porque su funcionamiento no era el óptimo y tenía un coste muy elevado.

En ese momento, y dado lo estratégico de dicho sistema, se decidió comenzar a desarrollar uno nuevo, aprovechando los avances de la tecnología surgidos durante esos años, que produjeron una bajada del coste de la parte hardware, y el conocimiento adquirido por el equipo de I+D. Este nuevo sistema de teleservicio se denominó Ear. El proyecto fue desarrollado entre los departamentos de I+D e ingeniería electrónica.

A la vez se pensó que en el caso de que surgiera el mismo problema que con teleservicio, esta vez el problema podía ser de mayor envergadura puesto que el parque de aparatos se incrementaba prácticamente en un 10% anual (la estrategia de la empresa en esta época consistió en apostar por la postventa en detrimento de la obra nueva comprando empresas más pequeñas y sumando parque de elevadores al existente). Y se decidió entonces comprar un producto comercial con un éxito contrastado y distribuido en España por una empresa que ofrecía un buen mantenimiento postventa. Se trató de la solución Dielro.

Por ello actualmente los tres sistemas de teleservicio conviven y cada uno de ellos funciona de forma autónoma, aunque los tres posteriormente vuelcan sus datos en el sistema CAT, donde se tiene centralizada toda la información.

En principio, teleservicio lleva ya alrededor de 5 años sin instalarse en ningún nuevo aparato. La tendencia natural del mismo es la de que vaya disminuyendo el parque de dicho sistema, pero mientras existan aparatos, debe mantenerse operativo. Se estima que actualmente está implementado en un 10% del parque de ascensores que tienen teleservicio.

Dielro y EAR se reparten el otro 90%, con una manifiesta superioridad por parte de EAR. Puesto que es una aplicación propia (con todo lo que ello conlleva en cuanto a control de la misma), con un funcionamiento más óptimo y con unos costes menores, se ha apostado más ella que por su competidora. La tendencia actual es la de continuar con los dos sistemas en un porcentaje de 80% para EAR y un 20% para Dielro.

En cuanto a las escaleras mecánicas, disponen de su propio sistema de teleservicio. Se trata de un sistema desarrollado en su totalidad por la empresa y que se instala en todas las nuevas escaleras. En general no se trata de un sistema tan crítico, puesto que en las escaleras nunca se realizan rescates. Simplemente se trata de que la escalera no está operativa, y que el cliente requiere su puesta en marcha a la mayor brevedad posible. Si es cierto que muchos grandes almacenes y alguna cadena de supermercados, junto con los aeropuertos, tienen contratos que obligan a la empresa a resolver las incidencias en unos tiempos menores de 4 horas en algunos casos.

Mientras tanto, el departamento de I+D continua investigando en el proceso de mejora continua del software de teleservicio, apostando sobre todo por la evolución de EAR y su adaptación a nuevas necesidades.

También es necesario tener en cuenta que el grupo empresarial, a nivel mundial, está tratando de buscar una solución global. De hecho actualmente hay un proyecto en marcha cuyo objetivo es la decisión de cuál debe ser el sistema de telealarma para todo el grupo en todo el mundo. Sin duda es un proyecto muy ambicioso y complejo, puesto

que además de la tecnología, hay que tener en cuenta las peculiaridades de cada país. Lo que puede valer para Belgica, es posible que en Angola sea realmente complicado de implementar.

2.1.2.1 Teleservicio

Se trata del sistema más antiguo y que ya no se instala en nuevos aparatos. Es necesario mantenerlo mientras exista parque con dicho sistema.

Figura 5

2.1.2.2 EAR

Es junto con Dielro uno de los sistemas más difundido en el actual parque de mantenimiento. Se trata de un sistema diseñado por la propia empresa, concretamente por el departamento de I+D.

EAR, puesto que ha sido diseñado a medida de unas necesidades concretas y desarrollado mediante equipos de proyecto formados por personal de varios departamentos, ofrece algunas características muy útiles para la gestión de telealarmas.

Figura 6

Por ejemplo, es capaz de interactuar con el CAT, de forma que este al recibir una alerta, es capaz de conectar directamente con uno de los técnicos que están de guardia. De esta forma, el tratamiento de la incidencia es mucho más rápido ya que la sincronización entre EAR y CAT hace posible avisar al técnico correcto. Además en la última versión se ha implementado un sistema de balanceo de carga de trabajo, de forma que la incidencia se asigna al técnico que menos trabajo tengan ese momento y que más cerca se encuentre del aparato que ha sufrido la avería.

Además EAR tiene otras funcionalidades, como detener un aparato en el caso de que no funcione la línea telefónica o en el caso de que el propio EAR esté averiado. De esta forma se evita que una persona se quede atrapada y no pueda avisar para proceder al rescate.

Otra característica importante que contempla es lo que se conoce como llamada prioritaria. Esta funcionalidad permite utilizar la línea de teléfono para otros usos, y en el caso de que haya una incidencia en el aparato, cortar todas las llamadas y dar paso a la de emergencia. La normativa obliga a que siempre que el ascensor esté en marcha, se pueda realizar la llamada. Esto es un gran ahorro para los clientes, puesto que no tienen que asumir mensualmente el coste de una línea de teléfono o tarjeta sim por cada aparato. Por ejemplo, con dos líneas se puede atender a 10 aparatos.

2.1.2.3 Dielro.

Este sistema pertenece a un tercero, se trata de un producto comercial. Está instalado en un buen número de aparatos del parque.

Ofrece una buena ventaja competitiva, puesto que es la única telealarma del mercado que no emplea ningún tipo de alimentación eléctrica ni baterías, garantizando lo exigido en la norma 81-28 por alimentarse exclusivamente de la línea telefónica de la red pública a la que se encuentra conectada y cumplir todos los requisitos relativos al factor de carga exigidos por el operador propietario de la red de telecomunicaciones.

Además permite que los operarios puedan utilizar el sistema de comunicación sobre y bajo la cabina, incluyendo pulsadores en ambos lugares. De esta forma permite establecer una conversación si el operario lo requiriese.

Figura 7

También permite comunicación desde el foso, utilizando una unidad con tecnología TRP (Transmitted Relay Process) que se conecta a la misma línea telefónica de la instalación en paralelo, como si se tratara de otra telealarma, ya que la llamada que se efectúe desde este terminal se identificará en el call center como "llamada de foso". Al ser tecnología TRP, no precisa energía adicional para su funcionamiento, solamente la proporcionada por la propia línea telefónica.

Otra funcionalidad es la comunicación con el cuarto de máquinas. Desde el interior de la cabina, así como sobre y bajo ésta, se podrá establecer una comunicación local con el cuarto de máquinas. Para ello será necesario disponer en dicho cuarto de un interfono específico. Puede conectarse utilizando

solamente los dos hilos de la línea telefónica que llega hasta la cabina.

La norma EN 81-72 determina que, en todos aquellos edificios que dispongan de un ascensor destinado al servicio de bomberos, deberá haber un sistema de comunicación específico entre la planta de acceso del bombero, la cabina y el cuarto de máquinas, que funcione según lo especificado en el artículo 5. 2 de la mencionada norma, cuando se produzca una alarma de incendio. Dielro dispone de una serie de complementos para dar cumplimiento a estos requisitos, en combinación con la telealarma Dielro.

Por otro lado, y en el caso de que el cliente solicite a la empresa la instalación de un sistema de ayuda a la audición para personas discapacitadas tal y como contempla la norma EN 81-28. En ese caso además la alimentación del bucle debe asegurar al menos 1 hora de conversación y es una característica que Dielro contempla.

Dispone además de su propio software de gestión de llamadas que ofrece muchas posibilidades. Por un lado, permite gestionar todas las llamadas de emergencia, tal como exige la norma EN 81-28. Por otro, se podrán atender todas las alertas procedentes de otros equipos Dielro, por ejemplo, los que había con anterioridad a la entrada en vigor de la norma EN 81-28. También se podrán atender llamadas de cualquier equipo del parque, independiente de la marca; aunque, no será posible disponer de todas las prestaciones que se obtienen cuando se trata de una telealarma Dielro.

2.1.2.4 Escaleras

Es un sistema distinto al de los elevadores. No es tan crítico, puesto que en las escaleras nunca se realizan rescates de personas atrapadas. Aunque en ocasiones, cuando el cliente es un supermercado o un aeropuerto, también pude que la avería sea urgente dada la criticidad para su negocio.

El sistema de teleservicio para escaleras ha sido también íntegramente desarrollado por la empresa, tanto la parte hardware como la parte software. Es un sistema muy similar a Ear aunque más sencillo, puesto que la normativa europea sobre seguridad en escaleras mecánicas no es tan exigente como en ascensores. Por ejemplo en escaleras no se requiere que haya un sistema de comunicación que sea atendido directamente en un Call Center, ni tampoco garantizar al menos una hora de conversación.

2.1.3 Servicios afectados por el plan

En este apartado se recoge el detalle de los servicios afectados por el plan: CAT, correo electrónico, datos de los usuarios del departamento CC24H, sistemas de teleservicio,…
Es fundamental la identificación de los servicios cuya contingencia deberá ser tenida en cuenta en el plan, y detallarlos al máximo para garantizar el éxito.

Una primera aproximación podría ser la siguiente:

CAT	Centro de atención telefónica. Vendría a ser lo que un call center o un servicio help desk en lo relativo a IT, para la gestión de las incidencias en el funcionamiento de aparatos elevadores, tanto ascensores como escaleras mecánicas. En este caso se trata de una aplicación que permite a los operadores registrar manualmente las incidencias que se produzcan en cualquier aparato incluido en el parque de mantenimiento, para posteriormente contactar con un técnico que pueda visitar la instalación y realizar la reparación correspondiente
Correo electrónico	El ya tradicional sistema de envío de correos utilizando un software cliente. En este caso el sistema que se utiliza es Exchange 2010 y como cliente Outlook 2010. Existe un buzón departamental donde se reciben avisos y averías, y también se utiliza para el caso de que haya que enviar documentación, de una forma mucho más práctica que utilizando el fax. En este caso el servicio sería el correo electrónico tanto interno como externo, que incluye la infraestructura de servidores de correo electrónico, la de comunicaciones, el dominio de Internet y los propios buzones, tanto el departamental, como los de cada uno de los
Mensajes a móviles	Aplicación integrada con el CAT que permite el envío de mensajes SMS a móviles para la comunicación bidireccional entre técnicos y operadores. Cuando se abre una incidencia en CAT, esta aplicación utiliza la de mensajería móvil para enviar un aviso al técnico correspondiente. Posteriormente la respuesta del técnico cuando finaliza la avería o rescate, llega también por medio de esta aplicación, que a su vez la traslada al CAT.
Datos del departamento	En este servicio se incluyen todos los documentos almacenados en el servidor de ficheros que el personal del departamento CC24h utiliza. Se trata de plantillas y modelos para el envío de documentación, horarios y turnos, y otra documentación. Están físicamente

	almacenados en una cabina de discos del CPD central y solamente tiene acceso el personal del departamento CC24H.
Fax	Aunque es un sistema cuyo ciclo de vida está próximo a su fin, debe mantenerse. En ocasiones hay que enviar información o recibirla de clientes que no disponen de correo electrónico, porque aunque se trate de un sistema obsoleto y de uso residual, debe mantenerse al menos a corto plazo.
Telealarma escaleras	Se trata del sistema de aviso cuando se produce una avería en alguna escalera. Es el equivalente a los teleservicios para ascensores. Cuando se genera alguna incidencia en una escalera, el sistema envía un aviso al CAT para indicar que dicha escalera tiene algún problema en su mantenimiento y debe revisarse y repararse en caso necesario
Telealarmas	Los tres tipos de telealarmas con los que funciona la empresa en lo relativo a ascensores son otro servicio que se verá afectado por el plan. Se trata de los sistemas que informan al sistema central del estado de los aparatos elevadores en cada uno de los momentos. En función de que tipo sea, proporciona más o menos información y hace uso de comunicaciones sms, correo electrónico o envio de datos por UMTS.
Llamada emergencia teleservicio	Aunque realmente es una funcionalidad de una de las telealarmas, se ha visto conveniente recogerlo como servicio independiente para tener en cuenta su criticidad de forma particularizada. Puesto que no es un servicio excesivamente crítico, no es conveniente mezclarlo con otros que sí lo son, y que estos se vean penalizados.
Acceso a Internet	Algunas de las operaciones diarias de contacto con los proveedores se realizan utilizando Internet. Por tanto es necesario que desde los puestos de los operadores se disponga del acceso a Internet. No se trata de un servicio muy crítico, puesto que también pueden realizarse las operaciones de apertura de incidencia o modificación de configuración por teléfono.

Tabla 2

2.1.4 Tiempos máximos asumidos sin servicio

En este punto se definen los tiempos máximos que el CC24H puede trabajar sin cada uno de los servicios. Además, se define la degradación de servicio tolerada, en la que se indican los mínimos para poder operar al menos durante los primeros momentos tras la contingencia. De esta forma, se trata de documentar la criticidad de los

servicios en función de su importancia para el correcto funcionamiento del departamento.

Para cada uno de los servicios los tiempos serían los siguientes:

- CAT

Se trata de uno de los servicios más críticos para el funcionamiento del sistema. Durante el tiempo que este servicio no esté operativo se podrá atender las incidencias desde las delegaciones, siempre y cuando la incidencia tenga lugar durante el horario laborable de las mismas. En general las delegaciones se encuentran operativas en horario de 8:00 de la mañana a 18:00 horas. Si durante ese horario ocurriera una incidencia, solo habría que tener en cuenta aquellas provincias en las que fuera festivo.

En el caso de que la incidencia tenga lugar fuera de dicho horario, el servicio debe darse desde el departamento CC24h y mientras el servicio no esté operativo no se podrá atender las incidencias. En este caso, la premura por la puesta en marcha del centro de respaldo es mucho mayor.

Se estima que el tiempo máximo asumible en recuperar el servicio sería de 8 horas en jornada laborable (de 8:00h de la mañana a 18:00h de lunes a jueves y los viernes de 8:00h a 14:30h) y de 4 fuera de dicho horario.
En menos de 4 u 8 horas (en función de si es o no horario laborable) se deberá disponer de los puestos de trabajo requeridos con acceso al sistema CAT en el centro de respaldo. Ello va a requerir que el procedimiento de puesta en explotación del centro de respaldo está muy bien definido. Cualquier error que se cometa en la planificación del mismo puede provocar que los tiempos requeridos no se puedan cumplir, provocando unos enormes daños económicos y de imagen a la empresa.

- Mensajes a móviles

El tratamiento de este servicio es el mismo que para el CAT. Es muy importante que los técnicos de mantenimiento y reparación de aparatos elevadores puedan ser informados de la incidencia que tienen que resolver de una forma automática, utilizando está aplicación desde CAT.

Si la aplicación de mensajes a móviles no está operativa, se puede contactar con los técnicos por teléfono. El problema de esté método es que debe realizarse de forma manual. Un operador del CC24h debe llamar al técnico y darle los datos. Y este, debe anotarlos mientras habla por teléfono, por lo que nos podemos encontrar con el problema de que no tenga forma de anotar.

La otra opción es enviarle un sms de forma manual, utilizando uno de los móviles disponibles de los operadores. En este caso el problema es el tiempo, puesto que el operador debe escribir a mano en el móvil el mensaje. Si solo es un aviso no es un gran problema, pero si se acumulan avisos se puede producir importantes retrasos.

Además se requiere de otra modificación adicional. Los técnicos cuando reciben el aviso por sms, acuden inmediatamente al lugar de la incidencia para tratar de resolverla. Una vez que la resuelven, envían un sms al número corporativo que se les indica. Este número está configurado de forma que cuando lo envían, llega directamente a la aplicación CAT. En el caso de que CAT no esté operativo en su centro principal, habría que desviar dicho número corporativo al número que corresponda a la nueva ubicación de la aplicación.

Por tanto, para la aplicación de mensajes a móviles los tiempos máximos asumidos sin servicio serían 8 horas en la jornada laborable (de 8:00h de la mañana a 18:00h de lunes a jueves y los viernes de 8:00h a 14:30h) y de 4 fuera de dicho horario

- Datos del departamento

Los ficheros de datos del departamento son también críticos, por lo que lo que los tiempos máximos de recuperación son los mismos que para el CAT: 8 horas en jornada laborable y 4 fuera de ella.

Dentro de los datos de departamento se encuentran todas las plantillas y modelos utilizados por el personal, para el envío de correos electrónicos, faxes, etc. Además de los horarios de turnos, los teléfonos de contacto e información adicional.

El volumen de dichos datos no es excesivo (alrededor de 4gb) por lo que su traslado, recuperación o copia de seguridad no conllevarían un tiempo excesivo.

- Fax

Se deberá de disponer de servicio de fax (a través de un fax físico en la ubicación de contingencia) en el tiempo que el operador de telecomunicaciones tarde en desviar el número, 4 horas aproximadamente. Será necesario disponer de un dispositivo de fax con su número para realizar dicho desvío.

En un futuro no muy lejano el fax dejará de ser un servicio crítico. Actualmente se está intentando sustituirlo por el correo electrónico, pero muchos de los clientes son reacios a utilizarlo. Por ello, y mientras este cambio se complete, el fax se continuará considerando crítico.

- Servidor Escaleras

Dado que las averías en escaleras mecánicas no provocan que una o varias personas se encuentren encerradas, este servicio no se ha considerado crítico. La avería de una escalera simplemente provoca que la misma se encuentre fuera de servicio, con los consiguientes trastornos para el cliente. Por ejemplo si se trata de una avería en una escalera de una estación de metro, los clientes siempre tendrán disponible las escaleras tradicionales y en la mayoría de los casos un ascensor para personas con problemas de movilidad. En el caso de que se trate de una escalera mecánica de un centro comercial, siempre existirá otra alternativa para pasar de una planta a otra, bien sea otra escalera, bien un ascensor.

Por lo tanto, se ha considerado que el servicio del servidor de escaleras es prescindible durante 24 horas a día de hoy. En el futuro este hecho cambiará, puesto que la tendencia del mercado está empezando a cambiar. Cada vez son más los clientes que solicitan un servicio de 24 horas en escaleras, con tiempos respuesta cortos, definidos por contrato. Cuando este hecho comience a extenderse, la criticidad de este servicio será otra distinta a la que tiene actualmente.

- Telealarmas (Test periódicos)

Aunque se trata de un servicio con gran relevancia para el departamento CC24h, se ha asumido que se puede prescindir de él durante al menos 24 horas. Ello es motivado porque las telealarmas envían las alertas cada tres días, por lo que la parada del servicio un día sería asumible.

Durante las 24 horas de la parada habría tiempo suficiente para poner operativos los servidores en el centro de respaldo y el servicio de telealarmas en el servidor de CAT, dando prioridad a los otros servicios, a los considerados más críticos. Durante ese tiempo, los mensajes enviados por los ascensores no se pierden, puesto que el centro de entrega de mensajes del operador los mantiene durante 48 horas. En general se tratará de mensajes que indican que el equipo elevador requiere algún tipo de mantenimiento, que sufre alguna avería que no requiere rescate, o que se encuentra correctamente. En el caso de que se trate de un rescate, la llamada pasará a través de CAT y no de las telealarmas, por lo que este servicio no es tan vital.

- Buzones de correo

Tanto el buzón departamental, como los buzones de los/as operadores/as deberán estar operativos en menos de 4 horas.

Este servicio se ha catalogado también como crítico puesto que por correo electrónico llegan numerosas incidencias en ascensores y en escaleras mecánicas. Además en caso de que haya que en enviar

algún documento, es un servicio mucho más flexible y cómodo de utilizar que el fax. En el departamento se dispone además de un escáner, por lo que cualquier documento es susceptible de ser escaneado y una vez en formato digital, se puede enviar donde sea necesario.

Se ha definido que antes de 4 horas debe estar operativo al menos el buzón departamental, que es utilizado por todos los operadores. El resto de buzones pueden esperar por encima de las 4 horas. Lo realmente imprescindible es disponer de al menos uno.

- Llamada de emergencia de Teleservicio.

Los elevadores que disponen de Telealarma ofrecen un servicio alternativo para realizar las llamadas de emergencia, desde el propio aparato.

Se ha decidido que se puede trabajar durante 8 horas sin este servicio, puesto que la persona o personas que se queden atrapadas en el ascensor, podrán realizar la llamada utilizando un móvil o avisar a alguien para que avise al servicio técnico desde fuera, utilizando el timbre del mismo. No es un servicio crítico, puesto que existe alternativa de funcionamiento sin él.

- Acceso a Internet.

Los equipos de los operadores del CC24H deben tener acceso a Internet. Es necesario para abrir incidencias con algunos de los proveedores, y también para solicitar cambios en las configuraciones. Por ejemplo, para el caso del proveedor de comunicaciones es muy importante tener acceso al menos al portal de dicho proveedor.
Como la comunicación con todos los proveedores puede hacerse por teléfono o por fax, no se considera un servicio excesivamente crítico aunque si importante. Es por ello que puede prescindirse de este servicio tanto en laborable como en festivo durante un máximo de 8 horas.

2.1.5 Recogida y análisis de requisitos

Detalla todos los requisitos del departamento CC24H para ofrecer su servicio en la ubicación de contingencia: equipos de operador, líneas de voz, fax,….

Los requisitos se dividen en requisitos de usuario y requisitos del sistema y el listado de requisitos obtenidos es el siguiente:

- RU01: El sistema CAT no puede estar fuera de servicio más de 8 horas en día laborable y más de 4 en festivo o fin de semana

- RU02: El sistema de envíos de mensajes a móviles debe estar operativo como máximo tras una parada de 8 horas los días laborables y de 4 los fines de semana y festivos
- RU03: Los ficheros de datos del departamento tienen que estar disponibles en menos de 8 horas en jornada laboral y menos de 4 horas los fines de semana y festivos.
- RU04: El servicio de Fax tiene que estar operativo en menos de 4 horas. Este requisito viene determinado por el tiempo que el operador de comunicaciones requiere para realizar el desvío de la línea original de fax a otra.
- RU05: El servidor de escaleras debe estar operativo en menos de 24 horas. Este requisito cambiará con el tiempo, por lo que de cara al futuro, será necesario tenerlo en cuenta.
- RU06: El servicio de Telealarmas debe estar operativo en menos de 24 horas, teniendo en cuenta que el operador almacena los sms durante 48h, esto garantiza que no se perderá información
- RU07: El correo electrónico, que incluye tanto los servidores, como las comunicaciones como los buzones del departamento debe estar funcionando en menos de 4 horas. Tanto en horario laboral, como en festivos y fines de semana, la criticidad es la misma.
- RU08: Las llamadas de emergencia de teleservicio deben estar operativas en menos de 8 horas.
- RU09: Desde los equipos de los operadores se debe disponer de un acceso a Internet y no se puede prescindir de él más de 8 horas.
- RS01: El CPD de respaldo debe estar al menos a 30km del principal.
- RS02: La oficina en el CPD de respaldo debe tener al menos cuatro puestos de operador
- RS03: El CPD de respaldo debe disponer de una centralita telefónica programable que soporte al menos 20 llamadas entrantes simultaneas
- RS04: El CPD de respaldo debe disponer de al menos 8 líneas de teléfono independientes de la centralita de las cuales al menos 4 deben ser digitales
- RS05: La centralita del CPD debe disponer de al menos 15 extensiones libres
- RS06: La oficina del CPD de respaldo debe disponer de un dispositivo de fax con su correspondiente línea
- RS07: El CPD de respaldo debe disponer de una versión actualizada del CAT, incluyendo su base de datos y aplicaciones auxiliares como envío de mensajes a móviles.

2.2 Resolución de incidencias parciales.

En este apartado se recogen los procedimientos de actuación en caso de averías parciales, es decir, aquellas en las que solo determinados servicios se ven afectados.

2.2.1 Fallo en el suministro eléctrico.

En el caso de un corte eléctrico, el sistema continuaría funcionando con el SAI del que dispone el edificio, con autonomía para una hora.

Si transcurrido ese tiempo el suministro eléctrico no se ha restablecido, sería necesario arrancar el grupo electrógeno que mientras tenga combustible diesel, proporciona energía al sistema. En caso de que el depósito diesel estuviera llegando a quedarse sin combustible y no hubiera certeza de que el suministro eléctrico ordinario fuese a estar operativo en breve, se podría gestionar con urgencia el pedido de más combustible diesel.

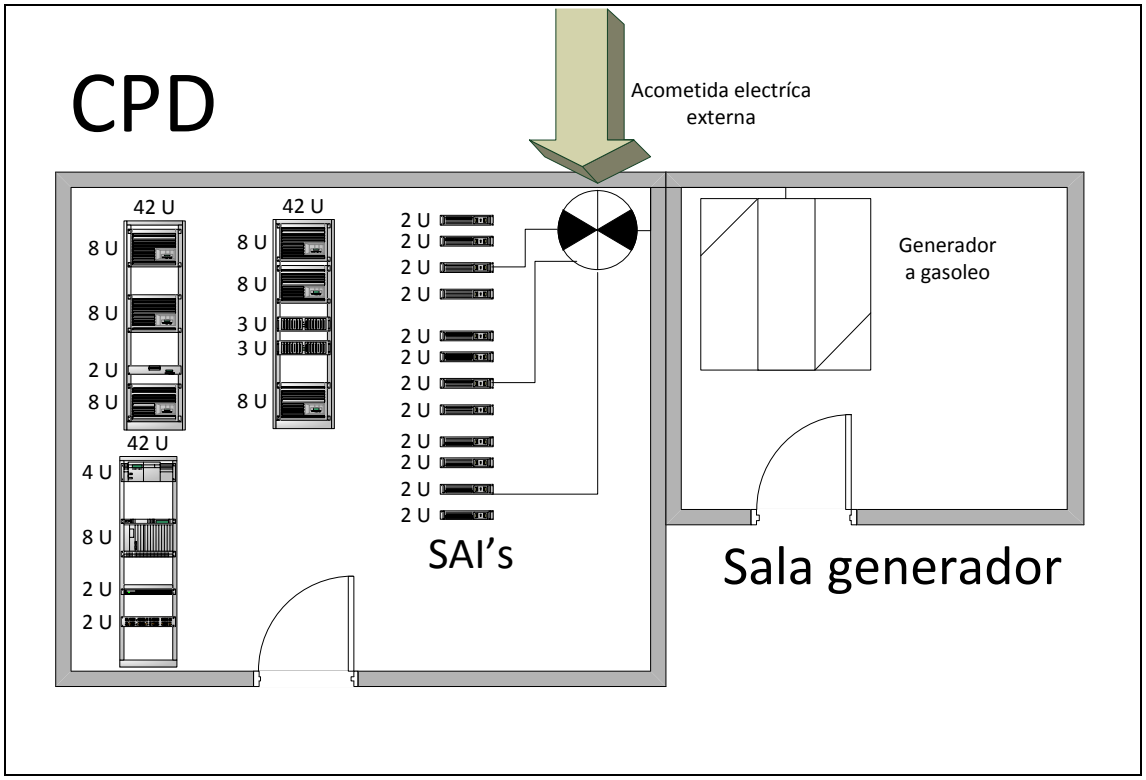


Figura 8

2.2.2 Avería en telecomunicaciones

En el caso de averías en las líneas de voz o datos, se abriría incidencia con el operador para que procediera a su reparación. En general las líneas no suelen tener averías con un tiempo de reparación muy largo, pero si este comenzara a serlo, se solicitaría al operador el desvío a las líneas de los teléfonos móviles.

Para el caso de las líneas de datos, existen además líneas de backup contratadas con el operador. En caso de caída de la línea principal, los datos podrían seguir llegando por medio de la línea auxiliar.

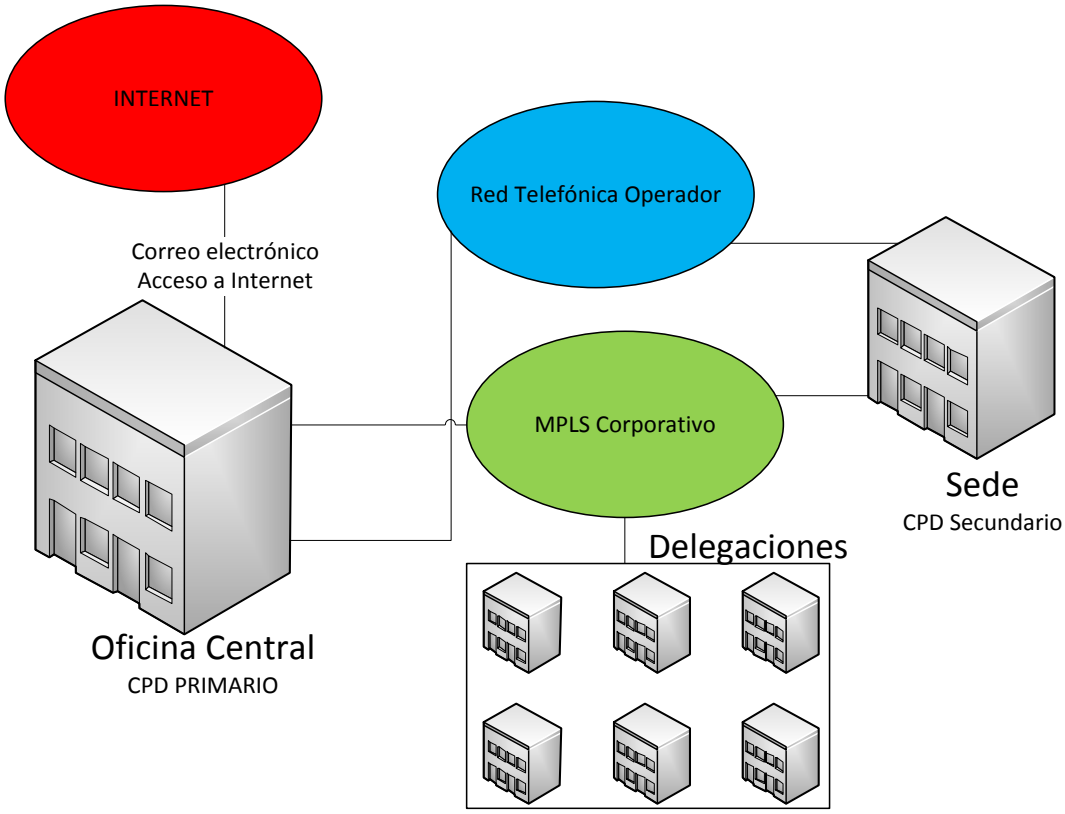


Figura 9

2.2.3 Avería en servidores de CAT

El servicio de atención telefónica se proporciona por medio de un clúster con dos nodos. En el caso de que se produzca una avería en uno de ellos, se pasa el control al otro y el sistema continúa funcionando con normalidad.

En el caso de que la avería se produzca en ambos servidores simultáneamente, se restauraría el servicio en otro servidor, a partir de una copia de seguridad. Por supuesto este procedimiento conlleva un trabajo y un tiempo de recuperación que deberá ser tenido en cuenta.

2.2.4 Avería en hardware de comunicaciones de telealarmas.

En el caso de que la avería se produzca en las baterías del modem de alguno de los tres sistemas de telealarmas, simplemente será necesario reemplazarlos por otros. El CC24H dispone de equipos de reserva de todos los sistemas. Esta sustitución se gestionaría como una reparación más del aparato elevador, incluso podría programarse

para el próximo mantenimiento manual del aparato, si no quedara muy lejos en el tiempo.

2.2.5 Avería en sistema de telealarma.

2.2.5.1 Teleservicio

El teleservicio se encuentra instalado en los servidores del CAT, por lo que el procedimiento en caso de avería es el mismo del punto 2.2.3

2.2.5.2 EAR

En el caso de que el servidor EAR se quede fuera de servicio será necesario restaurarlo de un backup. La restauración es sencilla y no requiere de grandes recursos hardware. Ello es debido a que EAR no mantiene los datos del parque de aparatos, lo obtiene de los servidores del CAT.

2.2.5.3 Dielro.

Para Dielro el procedimiento es el mismo que para EAR. Además en este caso al tratarse de un producto comercial, se dispone de soporte técnico del fabricante.

2.2.6 Avería en servicio de correo electrónico.

En el caso de que haya algún problema con el servidor de correo electrónico, este afectará tanto al correo electrónico de CC24H como a los buzones de los operadores/as.

El procedimiento consistirá en crear con la mayor celeridad posible nuevos buzones de correo en otro servidor que se encuentre operativo para que se continúen recibiendo correos con normalidad. Una vez realizado este paso, se procederá a restaurar los datos de los buzones a partir del backup más reciente que se disponga.

2.2.7 Contingencia en el envío de mensajes a móviles

El envío de mensajes a móviles se realiza desde un servidor independiente. En el caso de que dejara de funcionar, los operadores podrían enviar los mensajes manualmente desde el servicio de mensajería proporcionado por el operador de telefonía.
Mientras tanto, se procedería a restaurar el servicio en otro servidor, a partir de un backup.

2.2.8 Contingencia en servidores de datos

En el caso de alguna incidencia en los servidores que almacenan los datos de los usuarios de CC24H se procederá tal y como se indica en el punto 2.3. Puesto que los datos se encuentran contenidos en una cabina de datos en cluster, el procedimiento será el mismo.

2.2.9 Contingencia acceso corporativo a Internet

En el caso de que se produjera alguna incidencia con el acceso corporativo a Internet, en primer lugar habría que identificar en qué punto se localiza la avería. Puede ser una caída de la línea de comunicaciones, con lo que habría que contactar con el operador de comunicaciones y abrir una incidencia del servicio.
También podría ser algún problema en la infraestructura interna, bien en alguno de los puntos de la red local como switches o cableado de red, como en los equipos que proporcionan el acceso a Internet, el proxy Squid en entorno Linux o el firewall Checkpoint. Para cualquiera de los casos de problemas en la infraestructura local, la persona de contacto sería el ingeniero de telecomunicaciones, que es responsable de toda la infraestructura.

2.3 Recuperación del sistema completo

En este apartado se definen los procedimientos y requisitos para continuar proporcionado el servicio en el caso de una contingencia que inutilice todos los servicios, por ejemplo un incendio o una inundación en la ubicación física en la que se encuentren.
En el caso de este tipo de contingencia se supone que el servicio deberá proporcionarse durante un largo periodo de tiempo desde otra ubicación física distinta. Dicha ubicación podrá ser otra oficina de la empresa o un centro de respaldo externo, contratado con algún proveedor.

2.3.1 Requisitos de la ubicación física

La ubicación física desde la que opere el CC24H deberá tener una serie de características, algunas de las cuales serían las siguientes:

- Al menos 4 puestos de operador, deseables 8
- Una centralita telefónica programable
- Soporte para al menos 20 llamadas entrantes simultaneas, preferiblemente 30
- Al menos 8 líneas de las cuales al menos 4 digitales para identificar las llamadas
- 15 extensiones libres
- Línea de fax con dispositivo incluido

- Acceso al correo electrónico corporativo, tanto al buzón departamental como al de los operadores y resto de personal del departamento
- Acceso a Internet desde los puestos de los operadores.

2.3.2 Recursos humanos

En cuanto a RRHH serían necesarias las siguientes roles, algunos de ellos compatibles y por tanto acumulables en una sola persona:

- Responsable del plan → en cuanto se produjera la contingencia, sería inmediatamente avisado mediante llamada telefónica o mensaje de texto y con ello se daría por comenzado el plan. Sería el encargado de contactar con el resto de personas involucradas y de la coordinación. Debería ser una persona que conociera muy bien el funcionamiento de todo el sistema, las ubicaciones físicas y si fuera posible también a las personas.
  Además debería tener el poder de decisión suficiente para tomar decisiones complicadas en el caso de que fueran necesarias y la potestad de disponer de cuantos recursos (materiales y humanos) fueran necesarios.

- Ingeniero de hardware → será responsable de resolver todas las incidencias que puedan acontecer con el hardware. Ante cualquier incidencia con los servidores o equipos de los operadores deberá actuar para su pronta solución. En el caso de que no pueda resolver la incidencia por sus propios medios, deberá acudir al soporte técnico del fabricante con el que se dispone de un contrato de mantenimiento de los mismos. También será responsable de cualquier incidencia relacionada con la microinformática, con cualquier problema en los equipos de trabajo de los operadores.

- Ingeniero de sistemas → necesario para resolver contingencias relacionadas con los sistemas, modificaciones de la configuración,…
  Debería ser una persona de sólidos conocimientos técnicos, del sistema y de todas las arquitecturas que lo componen:
  - Sistemas operativos, en la plataforma Windows 2012 en este caso. En el caso de que se de alguna incidencia con el sistema operativo, debería ser capaz de resolverlo e impedir que el plan de contingencia quedara bloqueado.
  - Clúster de Microsoft, puesto que el CAT se aloja sobre uno. Se trata de un sistema tolerante a fallos con dos nodos. Uno de ellos actúa como maestro y el otro como esclavo y ambos roles son intercambiables. Como mínimo el ingeniero debería ser capaz de cambiar los roles en caso de necesidad y levantar el servicio del clúster en el caso de que hubiera sufrido una parada

- Sistema de mensajería y colaboración. En el caso que nos ocupa se trata de Exchange Server 2010. El ingeniero debería ser capaz de resolver incidencias relacionadas con el envío y recepción de correos electrónicos. Deberá mantener operativos los buzones de los operadores y el buzón genérico del departamento, además de asegurarse que se realice copia de seguridad.
- Relación con soporte técnico. En el caso de que se produzca alguna contingencia que no sea capaz de resolver, será capaz de ponerse en contacto con el soporte técnico de la aplicación o aplicaciones afectadas para su resolución a la mayor brevedad posible. En el caso de que la incidencia se localice en el CAT o en los sistemas de telealarma, deberá trabajar en equipo con el ingeniero de aplicaciones dándole soporte en lo relativo a los sistemas.

- Ingeniero de telecomunicaciones → encargado de gestionar todas las tareas que tengan que ver con comunicaciones de la LAN, dispositivos de la red, dispositivos de seguridad como firewall o dispositivos requeridos para el acceso corporativo a Internet, como proxys. Deberá ser una persona con experiencia, y que conozca bien la arquitectura de la red sobre la que va a trabajar. En caso de alguna incidencia con alguno de los equipos que no sea capaz de resolver, también gestionara la relación con el soporte técnico de los distintos dispositivos.

- Ingeniero de aplicaciones → un técnico que conozca el funcionamiento del CAT y de los sistemas de telealarma. En el caso de cualquier contingencia, deberá ser capaz de resolverla por lo que deberá ser un experto en dichos sistemas. Deberá conocer el código de las aplicaciones que han sido desarrolladas por la empresa por si en algún momento el fallo se localizara en las mismas y hubiera que realizar alguna modificación. Asimismo será capaz de poner en marcha cualquiera de los sistemas y de hacer de intermediario con el soporte de Dielro si el problema se localizara en dicho sistema.

- Responsable de telecomunicaciones → encargado de contactar con el operador de telefonía y comunicaciones, para realizar los pertinentes desvíos, contratación de nuevas líneas y demás servicios que sean necesarios. Deberá tener la potestad necesaria para poder contratar nuevas líneas tanto de telefonía como de comunicaciones a nombre de la empresa, por lo que tendrá una relación estrecha con los comerciales y técnicos de la operadora u operadoras.
  Este rol podrá recaer en la persona responsable del plan por ejemplo, puesto que no requiere de presencia física en ninguna de las instalaciones, aunque si puede requerir un gran esfuerzo en tiempo para completar la gestión o gestiones con el operador u operadores de comunicaciones.

2.3.3 Infraestructura del centro de respaldo.

Previamente a la elaboración del plan de actuación en caso de desastre total del centro principal, el centro de respaldo deberá disponer de una infraestructura que permita tener replicados los datos necesarios para agilizar la puesta en marcha. Por ejemplo, en el caso de la base de datos de CAT, se podría restaurar a partir de un backup. Pero es mucho más rápido tenerla operativa y actualizada en un servidor del centro de respaldo.

Por tanto, la infraestructura informática previa de que deberá disponer el centro de respaldo sería la siguiente:

- un servidor con el CAT actualizado → en este caso, y puesto que dicho servidor solo será utilizado en el caso de desastre grave en el centro principal, no se ha considerado necesario disponer de otro cluster. Con un servidor de tamaño medio del que se disponga de soporte técnico 24x7x2 será suficiente.

  Dicho servidor deberá tener al menos dos procesadores de cuatro núcleos cada uno a 2'7Ghz, 16Gb de memoria RAM y al menos 100Gb de disco duro. Será recomendable que la arquitectura del mismo sea de 64 bits, aunque no será imprescindible.

  En cuanto a tolerancia a fallos deberá disponer de una configuración de discos en al menos Raid 5, doble tarjeta de red y doble fuente de alimentación.

  Además, dicho servidor deberá incluir un sistema de copias de seguridad para respaldar todos los datos. En previsión de que el centro principal pueda estar fuera de servicio durante varios días o semanas, y teniendo en cuenta que durante ese tiempo, la ubicación secundaria será la principal, es necesario realizar copia de todos los datos, por si ocurriera alguna incidencia en el servidor de CAT.

  En el servidor estará instalado el sistema operativo Windows Server 2012, el servidor de bases de datos Microsoft SQL Server 2012 y la aplicación CAT, exactamente igual que el centro principal. Asimismo tendrá instalado y configurado el software de replicación desarrollado por la empresa mediante el cual todos los datos modificados por los operadores en el CAT, se sincronizarán con la base de datos de este servidor. De esta forma, cada transacción de la base de datos del sistema principal, se actualizará en el servidor del centro de respaldo. De esta forma se garantiza que en el caso de desastre del centro principal, en muy poco tiempo se puede continuar trabajando con CAT en el centro de respaldo.

De una forma gráfica, la replicación sería como se muestra a continuación:

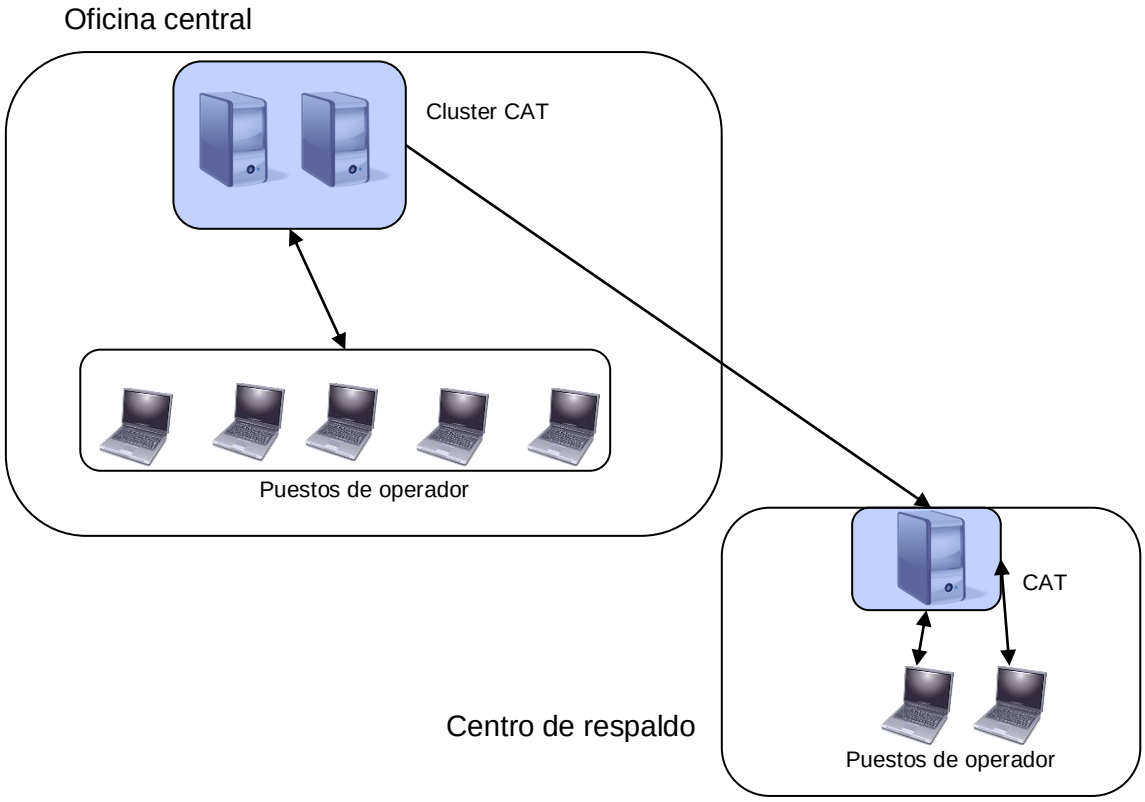


Figura 10

- Servidor para telealarmas. Se tratará de un servidor con las mismas características que el servidor para el CAT, pero en este caso dispondrá de cuatro máquinas virtuales, una para atender cada uno de los sistemas de telealarmas de que se dispone. La replicación de los datos desde el CPD principal se realizará por la misma línea de comunicaciones, tratando de realizarla en otro horario de forma que no se afecten entre ambas replicaciones. Las tres máquinas virtuales tendrán acceso al hardware, y se conectará para ello a la máquina física los correspondientes dispositivos de comunicaciones. Estos dispositivos no será necesario comprarlos, se utilizarán los que hay de reserva en el CPD principal.

- Línea de comunicaciones dedicada. En el centro de respaldo se dispondrá de una línea de comunicaciones dedicada para realizar la replicación de los datos. El ancho de banda de dicha línea no deberá ser inferior de 10 Mb/segundo y es importante que el caudal sea garantizado. Por ello se deberá optar por una solución MPLS, puesto que la tecnología ADSL no garantiza el caudal. Por el otro extremo, por la parte de la oficina central, la línea también deberá ser dedicada y con el mismo ancho de banda. Lo adecuado será introducir ambas ubicaciones dentro del anillo MPLS que el proveedor facilita a la

empresa, con los anchos de banda correspondientes. Con el proveedor de comunicaciones se firmarán SLA's que permitan garantizar la disponibilidad del ancho de banda requerido en todo momento.

- Centralita telefónica configurable: se requiere en el centro de respaldo una centralita digital que soporte al menos 20 llamadas simultáneas, que disponga de al menos ocho líneas de teléfono, cuatro de las cuales deberán ser digitales. Además, se deberá disponer de al menos 15 extensiones disponibles.
- Línea para el fax y dispositivo físico que permita el envío y recepción de faxes.

2.3.4 Plan de actuación

En este punto se detalla el plan de actuación, desde el momento en que se produce la contingencia, hasta que el servicio se encuentra totalmente operativo en otra ubicación física o en el caso de una incidencia parcial, hasta que el servicio afectado haya sido recuperado. También incluye el mantenimiento del plan y la adecuación del mismo a la normativa legal, así como la realización de simulacros.

2.3.4.1 Procedimiento

Para el detalle del procedimiento se explicará paso por paso y de forma detallada como puede verse a continuación:

- Paso 1 - Algún usuario o técnico detecta una incidencia en el sistema y se pone en contacto con el CAU.
- Paso 2 - El CAU abre una incidencia incluyendo la descripción facilitada por el usuario que la ha detectado.
- Paso 3 – Desde el CAU se contacta mediante llamada telefónica o sms con el responsable del plan.
- Paso 4 – El responsable del plan realiza una evaluación de la incidencia, y confirma si se trata de una avería parcial o total del sistema. En caso de avería parcial se continua el procedimiento por el paso 5 y en caso de avería total se continua en el paso 9

- Paso 5 – El responsable del plan verifica que tipo de incidencia parcial es la que se ha producido y contacta con el responsable del área afectada que puede ser el ingeniero de hardware, el ingeniero de sistemas, el ingeniero de aplicaciones o el responsable de telecomunicaciones
- Paso 6 – El responsable del área afecta realiza un análisis en profundidad de la incidencia. En caso de que pueda

resolverla por sí mismo lo hace y el procedimiento sigue por el paso 8.

- Paso 7 – El responsable del área afectada no puede resolver la incidencia por sí mismo. Contacta con el correspondiente servicio técnico, que es quién finalmente la resuelve e informa al responsable de área
- Paso 8 – El responsable del área contacta con el responsable del plan y le informa de que la incidencia ha quedado resuelta, tras haberlo comprobado. Se continua el procedimiento en el paso 16

- Paso 9 – El responsable del plan se pone en contacto con todos los responsables de las áreas: ingeniero de hardware, ingeniero de aplicaciones, ingeniero de sistemas y responsable de comunicaciones y les informa de que ha habido una incidencia que afecta a la totalidad del sistema, y es necesario comenzar a operar desde el centro de respaldo.
- Paso 10 – El responsable del plan contacta con el responsable del departamento CC24h para encargarle la coordinación con los operadores, indicándoles que deben trasladarse a la oficina aledaña al CPD de respaldo.
- Paso 11 – El responsable de comunicaciones informa al operador de comunicaciones de la incidencia, y el operador arranca su plan de contingencia. Inmediatamente desvía el número de atención telefónica ante averías en equipos elevadores a la centralita del CPD de respaldo. Se solicita asimismo el desvío del número de fax al número de la oficina del CPD de respaldo y el desvío de las llamadas de las telealarmas también a números de dicho CPD. El operador comprueba también que la centralita del CPD de respaldo se encuentra correctamente operativa y plenamente funcional para dar el servicio.
- Paso 12 – En paralelo, el ingeniero de sistemas revisa el funcionamiento del sistema de correo electrónico, del servidor de aplicaciones y de la base de datos. Asimismo, verifica que los datos están sincronizados correctamente al instante posterior al suceso de la incidencia en el CPD principal
- Paso 13 – También en paralelo, el ingeniero de hardware y microinformática comprueba que el servidor se encuentra en un estado óptimo y realiza pruebas con los pc’s de los operadores para comprobar que tienen correctamente configurado el acceso al correo electrónico y al resto de aplicaciones.
- Paso 14 – En paralelo a las anteriores tareas, el ingeniero de aplicaciones confirma que tanto el CAT, como los mensajes a móviles como el resto de aplicaciones están funcionando correctamente en el CPD de respaldo.

- Paso 15 – El responsable del departamento CC24h confirma que todos los servicios están operativos, y que el departamento está funcionando adecuadamente, teniendo en cuenta las restricciones de que el centro de respaldo dispone de menos recursos que el principal

- Paso 16 – El responsable del plan se pone en contacto con el CAU para informar de que la incidencia ha sido resuelta. Con la información que le ha facilitado el responsable de área, informa de los detalles de la misma
- Paso 17 – El CAU registra la información de resolución de la incidencia y la pasa a estado "pendiente de confirmación"
- Paso 18 – El CAU contacta con el usuario o técnico que abrió la incidencia y le indica que ha sido resuelta. Si no consigue contactarle, le envía un correo electrónico.
- Paso 19 – El CAU recibe confirmación del usuario de que la incidencia ha sido resuelta o trascurren más de 8 horas, la incidencia pasa a estado "solucionada"
- Paso 20 – Tras 72 horas sin recibir información de la incidencia, se pasa la misma a estado "cerrada". En caso de algún problema en la misma, el usuario puede volver a abrirla.

2.3.4.2 Mantenimiento del plan

En primer lugar será necesario definir un responsable del mantenimiento, que lo lógico es que sea el responsable del plan. Dicha persona será la encargada de seguir todas las pautas aquí definidas para garantizar la evolución del plan, en función de las nuevas necesidades que pueda surgir, o de los cambios que se produzcan. En importante tener en cuenta que el plan es algo vivo, susceptible de cambios con el tiempo. Y es vital para garantizar el funcionamiento del mismo, que todos los cambios que puedan afectar a dicho plan, se reflejen en el durante el mantenimiento que se realice.

El responsable del plan, será informado de cualquier cambio en las personas responsables de las áreas, en cualquier cambio que se realice de proveedor y de cualquier otro cambio que pueda afectar al plan. En los procedimientos del departamento CC24h se incluirá un apartado para que cualquier cambio que pueda afectar al plan, sea comunicado al responsable.

La forma más adecuada de garantizar la correcta evolución del plan sería realizar un simulacro, para comprobar que siguiendo la actual documentación del plan, se puede garantizar la continuidad del negocio. Pero la realización del mismo es complicada por varios motivos. El principal es el económico, la dificultad de encajar en unos presupuestos tan ajustados como los que hay actualmente en las empresas, unos costes que realmente no aportan a la empresa una mejora en su negocio. Está fuera de toda discusión

que un plan de contingencia que no funcione adecuadamente puede dejar el negocio sin continuidad, pero en ocasiones los directivos deciden asumir riesgos, para no incurrir en ciertos costes.
Por otro lado, está la dificultad de detener los sistemas para realizarlo. Evidentemente, el simulacro debe ser lo más real posible, y para ello hay que forzar la caída del CPD principal o bien detenerlo, y arrancar la ejecución del plan, con todos los inconvenientes que conlleva al negocio, especialmente al departamento CC24h y a su personal.

Por tanto, y dada la dificultad de verificar que se está realizando un buen mantenimiento del plan, y de que este sigue siendo válido en el estado actual, se propone la realización de una serie de acciones sencillas, que permiten verificar que las medidas del plan siguen teniendo vigencia, y que el plan está actualizado. En ningún caso dichas medidas son capaces de sustituir o garantizar la misma efectividad que un simulacro, pero dentro del compromiso entre servicio y coste, proporcionan una seguridad aceptable.

Las acciones que deberán realizarse para garantizar un buen mantenimiento del plan son las siguientes

- Realizar llamadas de teléfono a todos los contactos que aparecen en el plan. De esta forma se puede garantizar que las personas que asumían las responsabilidades siguen siendo las mismas y que su teléfono no ha cambiado. En el caso de que hayan cambiado, será el responsable del plan quien se encargue de identificar a la nueva persona, o el nuevo teléfono si es este el que ha cambiado. Sería conveniente realizarlo con una periodicidad mensual
- Verificar la replicación de datos entre el CPD principal y el de respaldo. Para el éxito del plan, es fundamental que los datos sean consistentes y estén replicados de la BD principal a la de respaldo, y que los datos están actualizados. Para comprobarlo simplemente es comparar los logs de transacciones de ambas BBDD, y ver que las operaciones que se realizan son las mismas, teniendo en cuenta el retardo de tiempo. Se recomienda realizarlo semanalmente, dado que es una tarea sencilla y poco costosa en tiempo.
- Comprobar que el backup de las aplicaciones y los datos se realiza correctamente. La mejor forma de verificarlo es restaurar los datos en un entorno de pruebas, que podría ser un entorno virtual. En dicho entorno se puede reproducir el entorno de producción de una forma sencilla y económica, y se puede comprobar que no hay problemas en la restauración. Para el caso de los datos, refiriéndonos a ficheros tal cual, es muy sencillo comprobarlo. En el caso de una base de datos o de alguna aplicación como alguna de las telealarmas supone una mayor carga de trabajo, pero es importante garantizar que se dispone de un backup operativo. Se recomienda realizarlo con una frecuencia bimensual.

2.3.4.3 Adecuación a la normativa del plan

La normativa a la que debe adecuarse el plan es aquella relativa a aparatos elevadores, y en concreto la relacionada con mantenimiento de los mismos y los rescates ante atrapamientos, que son las que puede afectar a la gestión de este plan de contingencia.

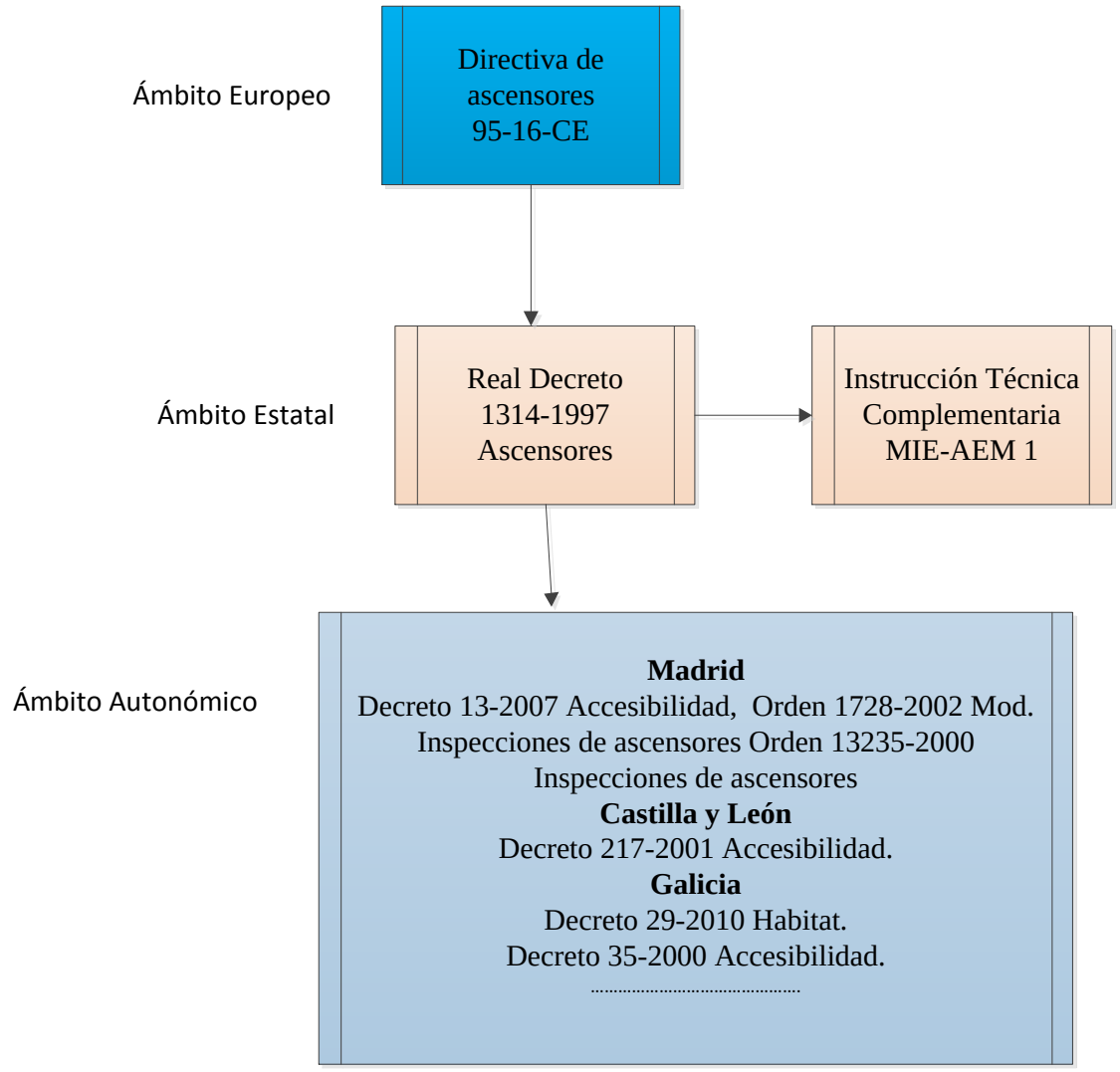


Figura 11

En concreto, la normativa legal que aplica sobre los ascensores en España, comienza por la de mayor rango, que es la normativa europea, la Directiva de ascensores 95-16-CE. En dicha directiva se especifican algunos de los requisitos para realizar el mantenimiento y rescate de un aparato elevador, y son los siguientes:

- Anexo 1, generalidades, punto 4 otros riesgos, punto 4.4: los ascensores deberán estar equipados con medios que permitan liberar y evacuar a las. personas retenidas en la cabina.
- Anexo 1, Generalidades, punto 4 otros riesgos, punto 4.5. Las cabinas estarán dotadas de un equipo de comunicación bidireccional que permita una comunicación permanente con un servicio de intervención rápida.

- Anexo 1, Generalidades, punto 6 instrucciones de uso, punto 6.2: cada ascensor irá acompañado de una documentación redactada en la lengua o lenguas oficiales de la Comunidad, las cuales podrán ser determinadas, de conformidad con el Tratado, por el Estado miembro en que se instale el ascensor. Dicha documentación constará como mínimo: de un manual de instrucciones y de de un cuaderno de incidencias, en el que se podrán anotar las reparaciones y, en su caso, las revisiones periódicas

El plan se adapta a toda la normativa de la directiva europea, puesto que respeta todas las obligaciones que emanan de dicha directiva.

En segundo lugar, la directiva que aplica es la nacional, en concreto el Real Decreto 1314-1997 Ascensores. Dicho decreto regula más en profundidad que la normativa europea y entra más al detalle en las medidas de seguridad de los aparatos elevadores y los controles que sobre los mismos deben realizarse. Asimismo, define como organismo competente el Ministerio de Industria para todas las autorizaciones relativas a la puesta en marcha de un nuevo aparato. En concreto en lo que al plan de contingencia afecta, serían los siguientes puntos:

- Anexo 1, punto 4 otros riesgos, punto 4.4 Los ascensores deberán estar equipados con medios que permitan liberar y evacuar a las personas
- Anexo 1, punto 4 otros riesgos, punto 4.5 Las cabinas estarán dotadas de un equipo de comunicación bidireccional que permita una comunicación permanente con un servicio de intervención rápida.

Adicionalmente al Real Decreto, la legislación sobre mantenimiento de ascensores y seguridad se encuentra definida con más detalle en la Instrucción Técnica Complementaria MIE-AEM 1, cuya última modificación data de febrero de 2013. En dicha normativa se especifican los siguientes puntos relacionados con este plan de contingencia,

- 5.3.2 plazos, especifica los intervalos máximos entre revisiones, que para la mayoría de los ascensores es de 6 semanas.
- 5.4 Obliga a la empresa mantenedora a mantener un registro de mantenimiento de cada ascensor del que es responsable
- 7.2 Garantizar, en plazo máximo de 24 horas, el envío de personal competente cuando sea solicitado por el titular o por el personal encargado del servicio ordinario del ascensor para corregir averías que ocasionen la parada del mismo, sin atrapamiento de personas en la cabina, y de manera inmediata cuando sean requeridos por motivo de parada del ascensor con personas atrapadas en la cabina o accidentes o urgencia similar.
- 7.4 Interrumpir el servicio del ascensor cuando apreciara riesgo grave e inminente de accidente, hasta tanto no se realice la oportuna reparación.

  Los cuatro puntos que hacen referencia al mantenimiento, son respetados por el plan de contingencia, puesto que permite el rescate inmediato de una persona atrapada, así como la visita para la solución de una avería en menos de 24 horas.

Por debajo de este Real Decreto y la Instrucción Técnica Complementaria en cuanto ámbito de aplicación, se encuentra la normativa de las comunidades autónomas. Por ejemplo, para el caso de la comunidad autónoma de Madrid, se aplica la siguiente normativa Decreto 13-2007 Accesibilidad, Orden 1728-2002 Mod. Inspecciones de ascensores, y Orden 13235-2000 Inspecciones de ascensores. En las tres se incluyen algunas modificaciones a la normativa estatal, como por ejemplo en la 1728-202 se recoge la obligación de instalar puertas en aquellos ascensores que no las tengan y también se incluye un listado de averías y el tiempo máximo que tiene el propietario para resolverlas en función de su gravedad.

En ninguna de dichas normativas se recogen artículos que puedan afectar a la elaboración del plan de contingencia, por lo que podemos asegurar que este se adecua a toda la normativa existente al respecto.

2.3.4.4 Simulacros.

Para la verificación del procedimiento, se realizaron dos simulacros. Uno de ellos, de una avería parcial del sistema, en concreto de fallo en el CAT y mensajes a móviles. Y el otro de una avería completa, dejando sin servicio desde el CPD principal, suponiendo que ocurrió un incendio en la oficina central

- Primer simulacro, avería en el sistema CAT y mensajería móvil.

El primer simulacro se realiza mediante un fallo del sistema CAT y de la aplicación auxiliar de mensajes a móviles. Se trata de una incidencia parcial en el sistema, aunque crítica puesto que son dos de los servicios fundamentales. Para realizarlo se eligió un domingo, en el que las delegaciones se encuentran cerradas y toda la atención a clientes se realiza desde las oficinas centrales del CC24H. Con respecto a la hora, se realizó comenzando a las 15:00h, una hora en la que se realiza el cambio de turno de operadores.

El simulacro comenzó con la parada controlada de ambos sistemas a las 15:00h, con lo que los operadores se percataron en cuanto se realizó el cambio de turno y comenzaron a entrar las primeras llamadas. Rápidamente, contactaron con el CAU, alrededor de las 15:04h, abriéndose una incidencia.

Siguiendo el procedimiento, desde el CAU se contactó con el responsable del plan, que fue informado de la situación. La información que recibió desde el CAU fue la recogida en la incidencia, en la que se indicaba que no había acceso al sistema CAT, y que los mensajes a móviles se estaban encolando en la bandeja de salida y que no llegaban a los destinatarios. El responsable preguntó por el resto de sistemas utilizados por el CC24H, pero desde el CAU no supieron responderle a dicha pregunta.

El responsable inmediatamente se puso en contacto con el ingeniero de aplicaciones, con el de sistemas y con el de telecomunicaciones. Los dos primeros respondieron al teléfono, y rápidamente se pusieron a trabajar en sus

respectivas áreas para tratar de encontrar el error y resolverlo. El responsable de comunicaciones no pudo ser contactado, no respondió al móvil.

Mientras los ingenieros trabajaban, el responsable del plan se puso en contacto con el CC24h para confirmar con los operadores el alcance exacto de la avería. Le indicaron que la incidencia se limitaba a los dos servicios indicados en la incidencia, y que el resto (correo electrónico, impresión, datos de departamento) no se habían visto afectados y que trabajaban con normalidad. Por el momento, estaban trabajando anotando las incidencias en una hoja de Excel compartida en el gestor de contenidos corporativo, Sharepoint en este caso. Al no disponer de acceso al CAT, la resolución y atención de incidencias estaba siendo más lenta, puesto que estaban teniendo que confirmar con los clientes los datos de cada aparato averiado. Por el momento no había habido ningún rescate, eran simples incidencias que se iban encolando a los correspondientes técnicos mediante llamadas de teléfono.

A las 15:25h el responsable del plan recibió una llamada del ingeniero de aplicaciones indicando que tanto el sistema CAT como la mensajería móvil se encontraban detenidos. El ingeniero los había puesto de nuevo operativos, y había realizado algunas pruebas, que habían finalizado con éxito. Se podía garantizar que ambas aplicaciones estaban de nuevo funcionando. El responsable de plan contacto entonces con el CAU para que se procediera a documentar la incidencia e informar al usuario que la había abierto. A las 15:35 el CAU estaba contactado con la operadora del CC24h que había abierto la incidencia para confirmar que la incidencia estaba resuelta y la operadora dio su visto bueno. Tras ocho horas sin que la incidencia fuera abierta de nuevo y sin tener ningún tipo de información al respecto, el CAU procedió a pasar la incidencia al estado solucionada y tras 72 horas más, se pasó a cerrada.

En global, el simulacro fue un éxito porque en un tiempo de menos de 40 minutos se pudo resolver la incidencia y conseguir que el sistema estuviera de nuevo operativo con todos sus servicios. Como puntos a mejorar, informar al CAU de que cuando abra una incidencia del departamento CC24h, se asegure de que cuales son los servicios que no se encuentran operativos. Es importante tener la información que permita discernir si se trata de una avería parcial que solo afecta a algunos sistemas, o si se trata de una incidencia completa.

También es importante informar a los técnicos de las distintas áreas que cuando tengan guardia relativa al plan de contingencia, estén atentos al móvil. En este caso el responsable de comunicaciones no respondió al teléfono, pero afortunadamente no se requirió de su intervención. Como mejora se propone que el responsable de plan tenga también la información de contacto de los diferentes proveedores y soportes técnicos, por si no fuera posible contactar con el responsable de alguna de las áreas.

- Segundo simulacro, incendio en las oficinas centrales.

Para la realización del segundo simulacro se eligió una avería total del sistema. Es decir, que el CPD principal y toda la oficina quedaran inutilizados para realizar el trabajo, y que ninguno de los servicios estuviera disponible.

Como día y hora, se propuso realizarlo en un festivo nacional, de madrugada, entre las 3:00h y las 4:00h de la mañana. Tras discutirlo con la responsable del CC24h y con el director del área técnica, se descartó dicha franja horaria, porque podría causar demasiado impacto en el servicio. Se propuso realizar el simulacro en un festivo nacional, pero por la mañana. Finalmente se acordó realizarlo a las 12:00h de mañana, un horario en el que habitualmente hay flujo de llamadas, pero que no es un horario punta en el que el tiempo requerido para el cambio de CPD y arranque desde el CPD secundario no sea tan crítico. Se asume por parte de la responsable del CC24h que el simulacro no se realizó en el caso peor, y que los tiempos obtenidos en este simulacro, pueden ser mejores que los que se obtengan cuando la incidencia se produzca en otro horario más crítico. Por parte del responsable del plan se asume que no es posible la realización del plan en un horario crítico y disponer de una medida del tiempo de recuperación en el caso peor.

A las 12:00 en punto del festivo elegio se realiza una parada de todos los sistemas del CC24h. A las 12:05h un operador del centro de control se pone en contacto con el CAU indicando que no pueden acceder al CAT ni enviar mensajes a móviles. El CAU pregunta por el resto de servicios, puesto que ha sido advertido de que es importante el mayor volumen de información posible y con el mayor detalle. Se le pregunta al operador por todos los servicios uno por uno, y se comprueba que ninguno está operativo. A las 12:10 el CAU registra la incidencia y se pone en contacto con el responsable del plan, que recibe la información de que ningún servicio está operativo. El responsable del plan realiza una evaluación rápida y al confirmar que se trata de una incidencia con parada total, comienza el procedimiento.

Inmediatamente, a las 12:15 el responsable del plan contacta con los responsables de cada una de las áreas por teléfono. Contacta con el responsable de telecomunicaciones, el ingeniero de hardware, el ingeniero de sistemas y el ingeniero de software. A todos les indica que se trata de una avería total del CPD y que se requiere proporcionar el servicio desde el CPD de respaldo, para que estén preparados por si fuera necesaria su intervención.

A continuación informa a la responsable del CC24h de la incidencia. Esta a su vez, contacta con los operadores de que deben trasladarse al centro de respaldo porque se va arrancar desde allí. A las 12:20 los operadores que se encuentra en la oficina del CPD central comienzan a trasladarse hacía el centro de respaldo. En paralelo la responsable del CC24h contacta con los operadores del siguiente turno para informarles que no se puede dar servicio desde el centro principal por una avería en todos los sistemas, y que deben comenzar su turno en el centro de respaldo.

A las 12:22 el responsable de comunicaciones se pone en contacto con el operador de comunicaciones y le informa de que debe iniciar el procedimiento interno necesario para trasladar todas las operaciones al CPD

de respaldo. Las tareas que debe realizar con más urgencia comienzan por desviar el teléfono de atención a usuarios al número de cabecera de la centralita del CPD de respaldo. También debe desviar el fax al número de la oficina de respaldo y las llamadas de las telealarmas, aunque estas no requieren la misma celeridad, puesto que lo importante es atender las incidencias.

A las 12:40 el operador ya tiene desviado el teléfono de atención al cliente y como los primeros operadores han llegado ya a la oficina de respaldo, se comienza a dar el servicio de atención telefónica desde allí. En estos 40 minutos, las llamadas han quedado grabadas en el buzón de voz del teléfono original, y los operadores las consultan. Solamente hay 10 llamadas, 9 son simplemente averías de diverso tipo de ascensores de comunidades de vecinos, algunos que han quedado detenidos en el bajo, otros entre dos pisos, luces fundidas, puertas que no cierran bien... La otra es más importante, puesto que se trata de una persona atrapada en un ascensor que ha llamado a las 12:17 y a la que hay que rescatar. Rápidamente uno de los operadores llama al técnico de guardia de la zona para que realice el rescate antes de las 13:17.

Mientras tanto el ingeniero de sistemas ha revisado el servidor de aplicaciones, la base de datos, el servidor de correo eléctronico y ha verificado que los datos se han sincronizado bien. La aplicación CAT en el CPD de respaldo tiene los datos correctos, no ha habido ninguna perdida en la sincronización y la última data de las 11:57, 3 minutos antes de que se produjera la parada.

En paralelo el ingeniero de hardware verifica que tanto los servidores, como los pc's de los operadores no tienen ningún problema físico. Además, en los ordenadores de los operadores comprueba que tienen configurado el acceso al correo electrónico, CAT y demás aplicaciones.

También de forma simultánea, el ingeniero de aplicaciones confirma que tanto el CAT como la mensajería móvil y demás aplicaciones están funcionando correctamente. Detecta que los mensajes a móviles no están funcionando y tras comprobar que no es un problema de la aplicación, se pone en contacto con el ingeniero de hardware que comprueba que se trata de un problema con la antena, y la reemplaza por otra. También verifica que las aplicaciones de telealarmas están ya preparadas para recibir notificaciones de aparatos elevadores.

A las 12:50h, el operador informa de que el fax ha sido desviado correctamente, por lo que puede utilizarse en caso necesario. Asimismo indica al responsable del plan que la centralita está plenamente operativa, y que si se desea algún cambio en la configuración, en el algoritmo de asignación de llamadas o en los mensajes automáticos, puede hacerse. El responsable del plan les indica que se ha detectado que la locución automática de respuesta no es la última versión, y se aprovecha para cambiarla y grabar la adecuada.

Asimismo, a las 12:55h el operador de comunicaciones indica que ya se han desviado los teléfonos de las telealarmas, y que los aparatos elevadores y escaleras mecánicas están ya realizando las llamadas al CPD de respaldo.

A las 13:15h los operadores confirman que tienen acceso a todos los servicios, incluidos aquellos que no son críticos, como puede ser el fax o el acceso a Internet.

En ese momento, el responsable del plan contacta con la responsable del departamento CC24h para solicitar confirmación de que el servicio ha sido restablecido y se encuentra 100% operativo. La responsable solicita tiempo para confirmarlo con el personal de su departamento, y las 13:30h responde afirmativamente. El responsable del plan le recuerda que hay ciertas restricciones en cuanto a rendimiento, puesto que la infraestructura del CPD de respaldo dispone de menos recursos que el CPD principal.

A las 13:35h el responsable del plan se pone en contacto con el CAU para indicar que la incidencia ha sido resuelta, y que se funciona con normalidad desde el CPD de respaldo. EL CAU registra la información relativa a la incidencia y la pasa al estado “pendiente de confirmación” y realiza una llamada al operador que abrió la incidencia, para disponer también de su confirmación. Con ello, la incidencia se cambia al siguiente estado, solucionada y tras 72 horas sin recibir ninguna notificación al respecto, se pasa a estado cerrada.

Este simulacro de incidencia completa, dentro de las limitaciones establecidas en cuanto a recursos del CPD secundario, se completó con éxito. Dicho esto, se recomienda ser cauteloso en su análisis, puesto que se realizó en un horario no crítico, eso sí, en un festivo de ámbito nacional en el que las delegaciones permanecen cerradas, y todo el tráfico de llamadas se desvía al call center central. En esta ocasión además, se consiguió contactar con todos los responsables de todas las áreas en las primeras llamadas, lo cual es un factor importante para conseguir el éxito.

Se aprovechó también para solucionar el fallo con la locución que se detectó en la centralita del CPD secundario, y se resolvió una incidencia con la antena utilizada para el envío de mensajes sms.

2.3.5 Varios

En este apartado se recogen algunas otras informaciones de interés para el plan que no han tenido cabida en otros apartados.

En el aspecto de la seguridad física, tanto en el CPD principal como en el secundario, el acceso se realiza por medio de una tarjeta de identificación y control de presencia. El sistema, que se gestiona por medio de una aplicación en un servidor corporativo, permite el acceso a cada una de las zonas de los edificios en función de los privilegios que se asignen a dicha tarjeta. Para este caso, será necesario garantizar que todas las personas implicadas en el plan tengan acceso tanto a los CPDs de ambas ubicaciones, como a las oficinas desde las que trabajaran los operadores. De igual forma, los operadores deberán tener acceso con su tarjeta a ambas oficinas.

Para ello, se deberá confirmar previamente con el responsable del departamento de Facility Management, responsable de dicho servicio. El teléfono de dicho responsable se incluirá en el plan, y se le facilitará información del plan, puesto que estará implicado en el caso de que ocurra alguna incidencia en el control de acceso. Adicionalmente, se facilitará al responsable del plan una llave de cada uno los cpd's y de las oficinas desde la que trabaja el personal del CC24h, que pueda abrir la puerta sin necesidad de tarjeta, por si ocurriera algún problema en el sistema de control de acceso que no pudiera resolverse de forma inmediata. De esta forma se garantiza el acceso a todos los espacios requeridos para el plan.

En el caso de que la incidencia total se produzca durante el cambio de turno, o no se consiga resolver con suficiente tiempo de antelación, será necesario informar del cambio de ubicación temporal al personal del siguiente turno. Para ello, se define en el procedimiento que será la responsable del CC24h la encargada de contactar con los operadores e indicarles que hay algún cambio en la ubicación en la que deben prestar el servicio.

2.4 Evaluación del plan de contingencia

2.4.1 Introducción

Una vez completado el plan de contingencia, será necesario realizar una evaluación del mismo, para comprobar si los objetivos iniciales se han podido completar con éxito. Antes de ponerlo en funcionamiento, es necesario comprobar que cumple las especificaciones y que se adapta al sistema actual.

En primer lugar, tenemos que verificar que es compatible con la estrategia actual. Es decir, realizar las comprobaciones pertinentes de que su implantación no afecta a otros sistemas, o a otras áreas de la empresa, y que sería posible realizar una transición desde la estrategia actual, hasta la

propuesta en el desarrollo de este proyecto, de forma que no se impactara al funcionamiento diario del departamento o departamentos afectados.

A continuación tenemos que realizar un análisis de la viabilidad económica del plan. Una vez analizada la compatibilidad y que los objetivos funcionales y técnicos se han cumplido, tenemos que comprobar que tanto el retorno de la inversión, como el coste que tendrá su implantación es asumible. Se trata de una ardua tarea, pero es necesario realizarla, puesto que es posible que la implantación del plan suponga un mayor coste económico que los beneficios del mismo.

A continuación se analizarán los simulacros realizados, para tratar de medir de una forma objetiva la posibilidad de éxito del plan una vez puesto en producción. Es cierto que no se pudieron realizar los simulacros en las condiciones que se deseaba, que en concreto era el caso peor, pero la realización de los mismos nos puede servir para tener una idea. La no realización de simulacros en el caso peor nos penaliza en cuanto a la medición de lo que sucedería en el caso real, pero nos favorece en la viabilidad económica, puesto que no incurrimos en los costes que tendría dicho simulacro.

Y por último, procederemos a la obtención de conclusiones globales de la evaluación que hemos realizado. Para ello tendremos en cuenta cada uno de los puntos que han sido analizados.

2.4.2 Compatibilidad con la estrategia actual

Para verificar la compatibilidad del plan con la estrategia corporativa actual, es necesario analizar el actual procedimiento de contingencias. Actualmente no se dispone de un plan global ante contingencias en los servicios del departamento CC24h. Cualquier incidencia que suceda en cualquiera de los servicios, se trata como una incidencia de cualquier otro tipo, no hay preferencia porque pertenezca a servicios de dicho departamento. Si es cierto que las incidencias, tal y como se gestionan desde el CAU, si tienen unos niveles de severidad definidos en función de cómo afectan al negocio. Pero son independientes del servicio, se pondera la criticidad de acuerdo a lo que afecte al negocio, no se tiene en cuenta el departamento al que afectan.

Por tanto, el plan es perfectamente compatible con la estrategia actual. Lo que se requiere es realizar una transición desde el procedimiento actual, al nuevo. Por ello, a partir del momento en que se ponga en explotación este plan, el procedimiento será el definido en dicho plan. A partir de dicho instante, cualquier incidencia relacionada con cualquier servicio que afecte al CC24h, tendrá un tratamiento especial por parte del CAU. Para ello, deberá seguir los procedimientos aquí definidos, que engloban un plan de contingencias completo para todos los servicios. De esta forma, se conseguirá agilizar la resolución de incidencias, y conseguir los objetivos marcados de restablecer el servicio dentro de los límites de tiempo aceptados.

2.4.3 Viabilidad económica

Para analizar la viabilidad económica de la propuesta, hay que analizar los costes en los que se incurre con la puesta en marcha y mantenimiento del plan, y enfrentarlos con los costes de no disponer de él. La comparativa se realizará en parte con estimaciones, puesto que no es posible conocer de forma exacta el coste que puede tener para la compañía la caída de servicios, en términos de imagen y posible pérdida de futuro negocio.

Para ello, se adjuntan estas tablas en la que se recogen los costes del plan, divididos en las correspondientes categorías

Infraestructuras

Recurso	Coste	Observaciones
2 Servidores con sistema de backup *	14645,15€	Se realiza compra del servidor y se realiza amortización del mismo a tres años
Dispositivo de fax	50€	Amortización a 5 años.
Centralita telefónica	5765,22€	El coste es anual, el alquiler a la compañía telefónica. Incluye mantenimiento y modificaciones. Incluye cuatro teléfonos digitales y cuatro analógicos
Líneas telefónicas, primario de voz	2330,12€	Las líneas se incluyen en la centralita y se gestionan desde ella. Este servicio lo da el operador, incluido en el coste de la centralita y una antena para envío de mensajes a móviles.
Línea fax	119,76€	Coste anual de la línea.
Comunicaciones MPLS, 10Mb/10Mb metropolitano	4490,16€	Incluye backup por ADSL 10Mb (10Mb/800Kb). Incluye alquiler de equipos
4 equipos para puesto de operador	4000€	El coste es la compra y se amortizan a 4 años.
Comunicaciones MPLS, acceso a Internet 10Mb (caudal garantizado 4Mb/500kb)	2327,19€	Incluye backup ADSL 10Mb (10Mb/800Kb) y alquiler de equipos.
2 licencias Windows Server 2012 standard	981,66	Precio con software assurance para un año.
1 SQL Server 2012 standard	1994,31	Precio con software assurance para un año.
1 Exchange server 2012 standard + 20 CALs	1911,59	Precio con software assurance para un año.

Tabla 5

Total anual infraestructuras al año: 25811,73€

* Características de los servidores: 2 procesadores Intel® Xeon® E7-4807 (6 core, 1.86 GHz, 18MB, 95W), 64GB (8x8GB) RDIMM, 2 tarjetas de red 1Gb NC375i Multifunction Ethernet Adapter 4 Ports per controller, 5 HD 300Gb, 6 G, SAS, 10.000 rpm, SFF. Incluye unidad para copia de seguridad LTO-6 Ultrium 6250.

Se requieren dos servidores:

- uno para la el CAT y el envío de mensajes a móviles. Incluirá la base de datos que se replicará desde el CPD principal con todos los datos
- otro para las telealarmas. Se dispondrá de una sola máquina física, y en ella se instalaran diferentes máquinas virtuales, una por cada tipo de telealarma: ear, dielro, telealarma y escaleras.

Adicionalmente a estas infraestructuras, se requiere de una ubicación física donde alojar todos los servicios. No se ha incluido en la infraestructura, puesto que se trata de una delegación de la compañía en la que hay espacio físico, y se aprovecha para reducir costes. En lugar de alquilar una nueva oficina, y aprovechando que en dicha delegación hay espacio por una reciente restructuración y traslado de personal a otra, se aprovechará para utilizarla con centro de respaldo. Además no es necesario realizar obras de adecuación, puesto que la oficina se encuentra habilitada. Se dispone de espacio para 10 personas, incluyendo el mobiliario que dichas personas requerirán para realizar su trabajo. Además se dispone de un CPD que cumple con la normativa de seguridad y que actualmente está en uso con dos servidores y una unidad de almacenamiento. El CPD dispone además de SAI, extinción de incendios, detección de agua y acceso securizado con tarjeta de empleado. Por ello, no hay que realizar ninguna otra inversión adicional, se dispone de la infraestructura necesaria.

Recursos Humanos

Función	Coste anual	Observaciones
Responsable del plan / Responsable telecomunicaciones	40.000€	Se estima que destinará un 20% de su tiempo al plan.
Ingeniero de sistemas	36.000€	Se estima que destinará un 10% de su tiempo al plan
Ingeniero de aplicaciones	37.000€	Se estima que destinará un 10% de su tiempo al plan
Ingeniero de hardware	34.000€	Se estima que destinará un 10% de su tiempo al plan
CAU	200.000€	Se estima que destinará un 2% de su tiempo al plan.
Responsable CC24H	40.000€	Se estima que destinará un 10% de su tiempo al plan.

Tabla 6

Para el coste de los recursos humanos se ha realizado una estimación del tiempo de su jornada anual que dedicaran a la generación y mantenimiento del plan, incluyendo el tiempo que tengan que trabajar en la resolución de incidencias. La estimación ha sido pesimista, teniendo en cuenta que el sistema en producción no tiene por qué fallar en condiciones normales, y que es complicado que ocurra un desastre en la oficina donde se aloja el CPD principal. Por ello, se ha estimado que el responsable de Telecomunicaciones en la empresa, que será el responsable del plan, solo dedicará un 20% de su tiempo. En el caso de los ingenieros, solo se requerirá de ellos un 10% de su jornada, el resto podrán dedicarlo a su trabajo habitual, igual que la persona responsable del CC24H. Por su parte, el Centro de Atención a Usuarios, se estima que solo dedique un 2% del total de tiempo anual a incidencias relacionadas con el plan, teniendo en cuenta que la compañía dispone de muchos otros servicios, como la microinformática, el ERP o la Intranet corporativa, que requerirán de mucho más tiempo para su gestión.

Coste total RRHH anual: 26.700€

Coste total anual proyecto= 26.700 + 25.811,73 = 52.511.73€

Por tanto, y una vez obtenido el coste anual del plan, es necesario estimar el coste de no tener dicho plan. Se trata de una estimación complicada, porque incluye parámetros tales como la pérdida de imagen o consecución de una imagen negativa como corporación, que son difíciles de medir. Asimismo, también habrá que evaluar la pérdida de confianza del cliente.

Por otro lado, será necesario tener en cuenta las pérdidas económicas directas, debidas a la pérdida de clientes por falta de satisfacción o las multas económicas que puedan ser impuestas por parte de las distintas administraciones, si por ejemplo no se realiza un rescate en el tiempo máximo permitido.

En cuanto a las estimaciones sobre los costes de no disponer del plan de contingencia, se han analizado teniendo en cuenta diferentes opciones. Por supuestos se trata de una estimación, porque el que estos supuestos tengan o no lugar, no depende de factores que podamos controlar: la reacción de un cliente particular (una comunidad de vecinos) ante un mal servicio, el no atender a una persona en un rescate en el tiempo adecuado y que ponga o no una demanda a la empresa (y lo que pueda ocurrir en el posible juicio), o el que ocurra alguna emergencia en una cadena de supermercados y el responsable de las infraestructuras decida no renovar el contrato. Todas estas situaciones escapan del control, porque dependen de las acciones u omisiones de otras personas. Se ha desglosado en diferentes supuestos, como se puede ver a continuación. En todos ellos se supone que ha sucedido una contingencia en el CPD y no se puede dar el servicio con garantías:

- Supuesto 1: avería en un ascensor residencial durante un domingo, que lo mantiene parado. Cuando se recibe la incidencia por teléfono, no se puede registrar en la aplicación por lo que los operadores deben tomar los datos a mano. Además, tienen que verificar los datos del ascensor, pero tampoco es posible comprobar si está al día

en el mantenimiento. Tampoco se tiene acceso a los técnicos de guardia en la provincia, ni a las tareas que están realizando. Por tanto se envía SMS a uno de ellos, indicándole los datos de la avería. El técnico lo recibe, pero está atendiendo otro aviso. La finca se queda sin ascensor durante toda la mañana y una parte de la tarde. El cliente llama varias veces enfadado e indica que va a romper el contrato por incumplimiento del mismo, de forma unilateral. Como se trataba de un contrato a 3 años, servicio oro con asistencia 24H se estaba facturando 1440€ al año, que se perderán durante los dos años y medio que faltan del contrato, con lo que la perdida asciende a 3600€ (1440€ en un año, que es como se está realizando la estimación). En este caso el daño para la imagen de la compañía es muy reducido, no va más allá del boca a boca entre los vecinos y familiares, se considera despreciable.

- Supuesto 2: avería en un ascensor residencial durante un festivo nacional, gestionado por un administrador de fincas que nos tiene contratado el mantenimiento de los ascensores de 30 fincas. La situación de avería es la misma que en el caso anterior. El problema en este caso es que el cliente es mucho más importante desde el punto de vista de nuestro negocio. En el caso de que los propietarios de la finca trasmitan su queja al administrador, este podría decidir rescindir el contrato, y no solo de dicha finca, sino de las treinta cuyo mantenimiento nos tiene contratado. En ese caso la pérdida estimada, y calculado como importe medio del contrato anual del ascensor 1130€, la pérdida anual sería de 33.900€. En este caso el daño a la imagen de la marca es mayor, puesto que son treinta comunidades de vecinos las que cambian de empresa de mantenimiento de ascensor. En una provincia pequeña, esto puede representar un problema, y estimamos que el coste para la marca puede estar en alrededor de 50.000€ por lo que el coste total es de 83.900€.

- Supuesto 3: rescate en un ascensor residencial durante un día laborable por la noche, a las 2:00AM. Estos rescates deben realizarse antes de una hora desde el momento en que se recibe en el CC24h la llamada. En este caso, la llamada se realizaría y es posible que no pudiera ser atendida, puesto que si la incidencia ha sido recientemente, podría ser que la centralita no estuviera operativa para recibir las llamadas, y aún no se habría conseguido desviar a un móvil por parte del operador. Especialmente en un día laborable por la noche, a pesar de que el servicio contratado con el operador sea de 24 horas, no se podría realizar con tanta celeridad. En ese caso sería imposible atender el rescate, y probablemente la persona atrapada llamaría al 112, servicio de emergencia, que enviaría a los bomberos para realizar el rescate. Por lo general, los bomberos saben cómo realizar un rescate, pero si por algún motivo el protocolo no les permite completarlo con éxito, no dudarán en forzar el ascensor, romper una puerta o lo que sea necesario. En este caso los costes para la empresa serían:

- Reparación del ascensor: entre 300 y 3500€, en función de las piezas averiadas para realizar el rescate.
- Coste de la salida de bomberos: que puede oscilar entre los 235 y los 1000€ en función de la ciudad o municipio. En principio los bomberos podrían reclamarlo a la comunidad de vecinos, pero la empresa mantenedora es responsable civil subsidiaria, por lo que sería responsable del coste.
- Demanda por daños y perjuicios contra la empresa de mantenimiento de aparatos elevadores. En este caso la estimación es más complicada, porque no hay unos baremos para la demanda, sería la parte actora la que tendría que poner en su escrito la cantidad que considera, pero fácilmente podría oscilar entre los 3000 y los 6000€.
- Pérdida del contrato del ascensor, valorada en 1440€
- Daño a la imagen de marca, cuando la noticia sea publicada en los medios de comunicación, probablemente solo a nivel local. Estimamos el coste económico en 100.000€, a partir de la experiencia con incidentes de este tipo.

Por tanto, para este supuesto 3, el coste total sería (utilizando medias de las estimaciones, excepto para los que se dispone del dato exacto) de 108.457'5€.

- Supuesto 4: avería en un elevador de una cadena de supermercados que tiene contratado el mantenimiento de todos sus ascensores (987) y escaleras mecánicas (137). La avería se produce en uno de sus supermercados principales, en el centro de una gran ciudad, uno de los que mejores rendimiento le proporcionan. El ascensor es utilizado para subir y bajar del parking con los carros de la compra, y se avería a las 12:00h de un sábado cuando se encuentra en hora punta. La avería impide que los clientes puedan bajar y subir con los carros de la compra, y tengan que utilizar la escalera. El responsable de mantenimiento del supermercado intenta contactar con el CC24h, pero ante la incidencia en el servicio, no lo consigue. Como se trata de un cliente VIP de la empresa de elevación, utiliza el teléfono móvil del comercial para informarle de la avería. Este se pone en contacto con el servicio postventa por medio de la responsable del CC24H. Esta le indica que hay una incidencia en el servicio, y que le enviará un técnico en cuanto sea posible. El gerente del supermercado en paralelo se pone en contacto con el responsable de grandes clientes, indicándole que es conocedor de la incidencia de los sistemas de la empresa, pero que necesita que le pongan en funcionamiento su ascensor a la mayor brevedad posible. El responsable de grandes clientes consigue contactar con un técnico de guardia, y enviarle al supermercado, pero han pasado casi dos horas desde que se paró el ascensor. El coste para la empresa en este caso se divide en dos partes:
  - Coste económico de indemnización: en el contrato con el supermercado están especificadas las penalizaciones por incumplimiento de contrato. En este caso, dos horas de

parada del elevador en un supermercado de los más importantes y en hora de máxima afluencia de público se penaliza con 100.000€.

- Coste en la imagen de la marca. Este coste es complicado de estimar, puesto que no tiene un efecto directo en la cuenta de resultados, pero si es cierto que supone un coste, y que podemos cuantificarlo haciendo una aproximación en 150.000€. Se trata de una cifra muy alta, pero hay que tener en cuenta que el cliente es muy importante por el volumen de contratación y pertenece a un sector en el que trabaja directamente con el cliente final, que puede ser cliente de la empresa en otra faceta de su vida, como en la laboral.

Por tanto, la empresa tendría que asumir un coste de 250.000€. Y ello sin considerar el peor caso, que sería que la cadena de supermercados decidiera romper el contrato por incumplimiento del mismo, o bien no renovar tras el siguiente vencimiento. En dicho caso, el coste para la empresa sería de varios millones de euros.

- Supuesto 5: avería en una escalera mecánica en un aeropuerto en un día laborable por la mañana. El aeropuerto tiene contratado el mantenimiento de todos sus ascensores (249) y escaleras (400 incluyendo pasillos rodantes), por lo que se considera un cliente VIP. Por las características físicas de la zona en concreto (falta de espacio), no se dispone de ascensor, la única alternativa es una escalera tradicional. Se trata de una zona de paso tras el control de acceso y equipajes, y antes de llegar a la zona de embarque. Los pasajeros solo llegan con maletas de mano, que por lo general pesan menos de 10kg. El responsable de mantenimiento de elevación del aeropuerto realiza una llamada al centro de atención a clientes, que ya ha podido ser desviada a móvil. Un operador toma los datos de la avería y trata de contactar con los técnicos asignados a soporte del aeropuerto. Como no tiene acceso a la aplicación, no puede saber quiénes son los que podrían atender la incidencia, y tiene que llamar a varios, hasta que consigue contactar con uno que puede atenderla. El técnico está en otra terminal del aeropuerto, por lo que entre el tiempo de llamadas y el desplazamiento, el técnico tarda casi 3 horas en llegar a atender la avería, más el tiempo que tarda en ponerla en funcionamiento, casi 5 horas sin escalera. El contrato de mantenimiento ha sido incumplido, porque obliga a la empresa a responder a cualquier incidencia en menos de una hora dentro de todo el recinto aeroportuario. Al no cumplirse dicho punto del contrato, el cliente penalizará el contrato con 70.000€ menos, que no representa una gran cantidad del total, pero si es considerable.

Por tanto, y si analizamos el retorno de la inversión (ROI) para cada uno de los supuestos, obtendremos la siguiente tabla:

Supuesto	Inversión Plan	Coste no plan	ROI
1	52.511.73	1440	-97%
2	52.511.73	83900	59%
3	52.511.73	108457'5	106%
4	52.511.73	250000	376%
5	52.511.73	70000	33%

Tabla 7

Como se puede apreciar en la tabla, el retorno de la inversión es favorable para todos los supuestos, excepto para el primero. Además es necesario tener en cuenta que un supuesto como el 1, de pérdida de un contrato de un ascensor por una mala calidad del servicio debida a no tener un buen plan de contingencia, puede ocurrir varias veces en un año. El ROI -97% lo obtenemos si solo perdiéramos un ascensor en todo el año, pero si no damos un buen servicio al cliente, probablemente perderemos muchos más contratos, además de futuras renovaciones no ejecutadas en las que el cliente cambie de proveedor. Por ejemplo, si durante un año nos ocurriera esta situación en 50 ocasiones (un porcentaje bastante bajo sobre un parque de 135.000 aparatos), el ROI sería del 37%, con lo cual ya tendríamos rentabilizada la inversión.

Como se puede ver en la tabla, es especialmente bueno el ROI en el supuesto 4, en el que no respondemos a las necesidades de un gran cliente. En este caso, la inversión en el plan está plenamente justificada, porque obtenemos un retorno de la inversión de unos 376% al ser capaces de satisfacer a un gran cliente, y que siga confiando en nosotros.

2.4.4 Simulacros

En el apartado 2.3.4.4 se recogen de forma detallada los simulacros que se realizaron de la aplicación del plan de contingencia. Se realizó un simulacro de incidencia parcial y otro de parada total de todos los sistemas. Ambos simulacros se completaron con éxito, con algunas pequeñas modificaciones ante problemas detectados, que se incorporaron al procedimiento definitivo.

De nuevo es necesario recalcar que por problemas de recursos, no se pudo realizar un simulacro en las condiciones peores, tal y como se deseaba. Es por ello que conviene resaltar que en el caso de una incidencia de este tipo, tanto los tiempos de respuesta como la resolución en tiempo y forma no sea la deseada. Pero este es un caso asumido tanto por la responsable del CC24h, como por la dirección de la compañía.

2.4.5 Conclusiones

Las conclusiones de la evaluación del plan de contingencia son positivas.

En primer lugar, hay que señalar que es compatible con la estrategia actual. Su implantación puede realizarse sin afectar a los servicios en

producción, ni a los actuales procedimientos de recuperación. Este ha sido uno de los requisitos tenidos en cuenta durante todo el desarrollo del plan. Es posible garantizar que la transición se realizará de una forma ordenada, y garantizando en todo momento la disponibilidad del servicio. Para ello se creará un plan de implantación que permita la adecuación de la organización al plan de la forma menos traumática posible.

Con respecto a la viabilidad económica, se ha demostrado que es absoluta. Dado el bajo coste del proyecto, tanto en infraestructuras como en recursos humanos, es una inversión muy pequeña para los beneficios económicos y la tasa de retorno de la inversión que tiene. Los beneficios que se obtienen de disponer de un plan de contingencia para uno de los servicios más críticos que la empresa está obligada a ofrecer, hacen de este proyecto una necesidad a corto plazo.

Por tanto, desde el punto de vista económico y financiero es un plan perfectamente viable.

Desde el punto de vista de los simulacros, también hemos visto que es perfectamente viable, y que han funcionado con razonable éxito. Además, han servido para pulir algunos de los aspectos del mismo de forma que el coste de los mismos, ha sido rápidamente amortizable.

Por tanto, podemos concluir que es un proyecto viable. Se trata de una inversión pequeña, que puede reportarnos grandes beneficios. En el caso de que ocurra alguna incidencia, por pequeña que sea, ya prácticamente se cubre el coste de la inversión con el dinero que se dejaría de percibir en caso de no implementar el plan.

3 Objetivos

El Plan de Contingencia, también llamado Plan de Continuidad del Negocio es un modelo de análisis de los posibles problemas que puedan tener lugar en un CPD, o en un ámbito más amplio, que sería el de los servicios informáticos en su totalidad. Algunos de estos problemas o incidencias podrían llegar a denominarse desastres, bien por su coste económico directo, bien por las consecuencias sobre la satisfacción de los clientes, bien por la pérdida de liderazgo en el mercado a medio o largo plazo.

El Plan de Contingencia pretende ser el soporte de la compañía en el caso de producirse alguna emergencia que influyera en la suspensión del servicio ofrecido por ella. Un plan de contingencia es el proceso que determina cual es el procedimiento cuando ocurre una catástrofe en la organización y es necesario recuperar algunos de los sistemas.

En el caso concreto de este proyecto, el alcance no es la totalidad de los sistemas de la empresa, solamente los servicios requeridos para el funcionamiento de uno de sus departamentos, en concreto el departamento CC24H. Es necesario señalar que no se trata de un departamento más. Es el que realiza el seguimiento técnico de averías y rescates sobre la totalidad de los aparatos del parque de mantenimiento. Y el mantenimiento de aparatos, es la parte del negocio que más dinero genera. Dada la actual crisis de la construcción, la obra nueva apenas genera actividad económica. Y es en el mantenimiento de aparatos, donde se pueden obtener beneficios.

Al desarrollar este plan de contingencia se pretende reducir al mínimo la posibilidad de que se produzcan problemas en las infraestructuras y datos, que pueda provocar una pérdida económica a la empresa:

- Instalaciones e infraestructuras: Se debe hacer de las infraestructuras de la organización un lugar seguro de forma que ante incidencia, se pueda mantener el servicio.
- Datos: En cuanto a los datos, se requieren técnicas de prevención y recuperación para asegurar la integridad y disponibilidad de los mismos.

Para cumplir este objetivo se han de implantar las medidas establecidas en el plan de forma inmediata. En el procedimiento se definen las operaciones necesarias que se deben realizar y la secuencia correcta de las mismas para restablecer por completo el funcionamiento de los sistemas afectados por la incidencia.

El objetivo de este plan de contingencia, es asegurar la capacidad de supervivencia de la empresa, en este caso del departamento CC24h, ante eventos que pongan en peligro sus servicios

Se debe reducir la probabilidad de fallos en el servicio a un nivel mínimo aceptable, con un coste razonable y asumible, y asegurar la adecuada recuperación de todos los servicios en un tiempo previamente definido.

Se quiere asegurar que existan controles adecuados para reducir el riesgo por fallos o mal funcionamiento de los sistemas.

Para conseguir el correcto desarrollo y una efectiva implantación del plan de contingencia en la organización, todas y cada una de las personas implicadas deben estar concienciados con el compromiso de la participación en la ejecución del mismo.

Para que se puedan llegar a cumplir por completo el objetivo del desarrollo del plan de contingencia, es necesario que se cumplan una serie de requisitos. Entre estos requisitos se podrían definir como los más importantes los siguientes:

- acometer una recogida de información en la que se detalle qué operaciones se han de realizar y quiénes son los encargados de realizar cada una de estas operaciones. Esta información deberá reflejarse de forma que en el caso de una incidencia, cada persona sepa cuáles son sus obligaciones.
- Definir un plan para la recuperación de cada uno de los servicios. Este plan deberá ser independiente para cada uno de ellos, lo que facilitará poner en funcionamiento los mismos. Además debe existir un plan global para el caso de una contingencia que afecte a la totalidad de los servicios del departamento.
- Se documentará de forma detallada el procedimiento de recuperación y una fase posterior de pruebas del sistema una vez que se haya producido la incidencia.
- Este plan deberá distribuirse a todos los empleados afectados de la organización, de tal forma que esté totalmente accesible a todo el personal encargado de la recuperación de los sistemas.
- Además, el plan debe contemplar una fase de validación de las operaciones realizadas para la recuperación de un desastre.

Los objetivos que se plantean con la elaboración de este proyecto se pueden resumir en uno principal: garantizar el funcionamiento del CC24H ante cualquier tipo de contingencia que pueda surgir. Tanto si se trata de una incidencia parcial en alguno de los sistemas, como si se trata de una avería total, el plan será capaz de mantener todos los servicios operativos. Se trata de un departamento estratégico de la empresa, puesto que su gestión de los mantenimientos de los aparatos elevadores y su capacidad para responder con rapidez a las posibles incidencias en los mismos, son una parte muy importante para el objetivo de conseguir la satisfacción del cliente.

Para conseguir el éxito en la persecución de este objetivo son necesarios planes para las siguientes contingencias:

- Contingencia ante desastre parcial: se trata de aquel que solo afecta a un servicio de los requeridos por el CC24h. Se definirán planes de recuperación por cada uno de los servicios de forma individual. De esta forma, una vez identificado el fallo en un servicio, se podrá trabajar inmediatamente sobre el siguiendo el procedimiento. De esta forma la recuperación del sistema se realiza de una forma más

rápida, a la vez que se optimizan recursos porque no se requiere de la participación de todo el personal definido en el plan, solamente de aquél directamente implicado en el sistema que presenta la incidencia.
Además tendremos que definir unos tiempos de parada de servicio máximos, antes de los cuales tendremos que ser capaces de restablecerlo. Esta es otra ventaja de disponer de planes individuales por servicios, que tendremos la flexibilidad de definir diferentes tiempos máximos de restauración en función de la criticidad del servicio.

- Contingencia ante desastre total: se trata de aquel que afecta a todos los servicios del departamento CC24h. En este caso ningún servicio está operativo, porque la propia infraestructura que los soporta ha sufrido un daño. En este caso si será necesario movilizar todos los recursos del plan, de forma que puedan trabajar en paralelo cuando sea posible, para conseguir la restauración del sistema en cuanto sea posible.

4 Entorno de Trabajo

En este apartado se recoge el entorno de trabajo tanto a nivel software como a nivel hardware. En él se detallan los diferentes sistemas operativos y aplicaciones de los que deberemos disponer en nuestra plataforma para que los servicios del departamento CC24h estén funcionando. También se tratará de estandarizar las versiones en todos los dispositivos, para evitar problemas de compatibilidades.

En cuanto a las versiones del software, se intentará mantenerlas en la última versión posible, realizando previamente pruebas de compatibilidad entre los diferentes software a utilizar. Para ello se creará un entorno de desarrollo y otro de pre-producción utilizando máquinas virtuales. Antes de realizar alguna actualización en producción, se probará previamente en el entorno de desarrollo, y posteriormente en el de pre-producción, que deberá ser una imagen lo más fiel posible al entorno que se está explotando. En dichas operaciones se implicará al personal que trabaja en el proyecto, puesto que es el que mejor conoce el entorno.

Con respecto al hardware, se cuenta con un clúster de servidores conectados por el sistema fibber-channel a una cabina de discos donde se ejecutan las aplicaciones fundamentales del CC24H: CAT y mensajes a móviles. En dicho clúster además corre el servidor de base de datos donde se almacena toda la información relativa a la gestión de incidencias y mantenimiento de los aparatos elevadores. Los servidores son de tamaño medio, aunque si incluyen algunas características avanzadas, como la gestión remota por conexión ILO, el cambio por avería y la ampliación de hardware en caliente, entre otras.

Además se dispone de servidores adicionales para el correo electrónico y para las telealarmas y otros hardware menores para el resto de servicios.

4.1 Software

Con respecto al entorno software en el que vamos a trabajar, podemos hablar de un entorno homogéneo con productos Microsoft. La sencillez en el manejo de las aplicaciones de este fabricante, junto con su posicionamiento líder en el mercado tanto privado como particular, ha hecho que tanto sus sistemas operativos como sus aplicaciones de ofimática o incluso de servidor, sean muy utilizadas. Además, la sencillez en la operación junto con sus costes ajustados, ha hecho que el retorno de la inversión de estos productos sea muy bueno. Por otro lado, su gran implantación en todos los mercados, de casi monopolio en algunos de ellos, ha provocado la compatibilidad tanto con clientes como proveedores, aunque está amenazada por otros productos que ofrecen ya esa misma compatibilidad.

La lista del entorno software sería la siguiente:

- Sistemas operativos de servidor: plataforma Windows, el 90% con Windows Server 2012 y el 10% con Windows Server 2008.
- Sistemas operativos de cliente. Entorno Windows con la siguiente distribución aproximada en el parque de equipos:
    - Windows 8: 20% del parque
    - Windows 7: 70% del parque
    - Windows XP: 10% del parque.

  NOTA: Windows XP no tiene soporte del fabricante desde abril de 2014. Esto implica que no se distribuyen parches de seguridad para dicho sistema operativo y que una vulnerabilidad no encontrada hasta ahora, podría comprometer la seguridad del equipo.

- Servidor de correo electrónico: Exchange Server 2012 (90%) y Exchange server 2010 (10%)
- Servidor de base de datos, para almacenamiento de los datos de mantenimiento del parque, datos económicos, aplicaciones de gestión e intranet: SQL Server 2012
- Paquete ofimático para equipos sobremesa y portátiles (Office 2013,10%, Office 2010, 80%, otras versiones 10%)
- Software para la gestión de incidencias relacionadas con los aparatos elevadores: CAT (centro atención telefónica, incluye servidor y puestos de operador). Se trata de una aplicación desarrollada de forma interna y cuyo mantenimiento y evolución lo realiza un equipo técnico de la propia plantilla de la empresa. La aplicación almacena toda la información en una base de datos y contiene toda la gestión de averías y labores de mantenimiento realizadas sobre los aparatos, incluyendo los rescates.
- Telealarmas: Teleservicio, escaleras, Dielro, EAR. Se trata de las aplicaciones que gestionan de forma automática los mantenimientos de los aparatos elevadores. Automáticamente envían información del estado del aparato, con el objetivo de poder realizar un mantenimiento preventivo.
- Mensajes a móviles. Se trata de la aplicación independiente, pero integrada en CAT, que permite enviar mensajes SMS a los técnicos de mantenimiento para pasarles datos de averías o rescates en equipos elevadores

4.2 Hardware

Con respecto al hardware, hay una parte genérica de servidores, cabinas de almacenamiento, fax y telefonía, y una parte específica para las comunicaciones con los aparatos elevadores. Cada aparato incluye un hardware de comunicaciones (modem), que le permite enviar información del estado en que se encuentra, si ha detectado alguna avería, si necesita revisión……

El listado del hardware sería el siguiente:

- Servidores clúster con cabina de discos. Se trata de los servidores que alojan la aplicación CAT, la aplicación de mensajes a móviles, y su base de datos. Son servidores potentes, con redundancia en fuentes de alimentación, 4 procesadores de 4 nucleos, 32gb de RAM y con la última tecnología hardware, incluyendo sustitución y cambio de hardware en caliente, tarjeta para acceso remoto por hardware,.. Con respecto a la cabina de discos, se utiliza una SAN, conectada a ambos servidor por fibre-channel.
- Servidores de tamaño medio para Telealarmas. Para los sistemas telealarmas, dielro, ear y para escaleras mecánicas, cuatro servidores de tamaño medio, uno para cada uno de los sistemas. Se trata de servidores con dos procesadores de cuatro núcleos, 8gb de RAM y 800gb de almacenamiento en disco. Aunque el parque de aparatos es grande, la información que se almacena es texto plano en bases de datos propietarias, que posteriormente y de forma automática se vuelcan en la base de datos de CAT.
- Servidor tamaño grande para correo electrónico. Al igual que para los servidores del clúster de CAT, para el servicio de correo electrónico, y dado el gran volumen de buzones de que dispone, además de los del personal de CC24h, se requiere un gran servidor. Las características del mismo son similares a las de los servidores de dicho clúster.
- Cabina de almacenamiento. Para los datos del departamento, y para el resto de datos del personal de la misma oficina de la compañía, se dispone de una cabina de almacenamiento. En este caso se trata de una cabina NAS, conectada a la red como un dispositivo más, y de la que se hace backup sobre otra NAS.
- Baterías de modem para Telealarmas. Para los cuatro sistemas de telealarmas se requieren baterías de modem conectadas a cada servidor, y que reciban las llamadas de los aparatos elevadores y pasen los datos al servidor. Cada uno de los sistemas, dispone de su propia batería de módems.
- Teléfonos digitales. Se trata de teléfonos que permiten la identificación del llamante, entre otras funciones avanzadas de telefonía. Se requiere de líneas digitales en la centralita y de dispositivos físicos con funciones digitales.
- Dispositivo de Fax. Aunque es un sistema de comunicación en franco desuso y que está siendo sustituido poco a poco por otros, aún se sigue utilizándose de forma residual. Requiere de dispositivo físico y línea de fax.
- Proxy para el acceso corporativo a Internet: dispositivo hardware conectado a la red que permite la conexión a Internet. Realiza diversas funciones, como la optimización del ancho de banda mediante cacheo de información, el control de acceso a los contenidos, el control de acceso de usuarios y el anonimato de los mismos en el acceso.
- Firewall perimetral para protección de la red. Puesto que la red local tendrá acceso a Internet por medio del proxy, se dispone

de un firewall para securizar dicho acceso. El firewall realiza las opciones de securización de la infraestructura, filtrado de accesos, detector de intrusiones y acceso remoto a la infraestructura por VPN.

5 Método de Resolución

5.1 *Introducción*

Para el desarrollo de un proyecto siempre es necesario seguir los estándares, tanto internacionales como los del propio país donde se ejecuta el proyecto. En el caso que nos ocupa, el de un plan de contingencia, hay una serie de estándares que se ha utilizado, y que se detallan a continuación.

La realización de este proyecto se ha realizado conforme a las siguientes normas:

- UNE 71599:2010 – Gestión de la continuidad del negocio, dividida en dos partes:
  - UNE 71599:2010-1 Código de práctica
  - UNE 71599:2010-2 Especificaciones

El objetivo de esta norma en sus dos partes es el de proporcionar la base para la comprensión, desarrollo e implantación de la continuidad de negocio en una empresa. Además, trata de proporcionar a los clientes y a otras organizaciones la confianza necesaria para el desarrollo de negocios. Permite también a una corporación medir su capacidad de garantizar la continuidad del negocio de una forma coherente y objetiva.

- ISO 22301 Bussines Continuity Management System. Dicha norma, identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso a seguir, los principios y la terminología de gestión de continuidad de negocio

Figura 12

La norma ISO 22301 es capaz de proporcionar una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de cualquier organización, independientemente del tamaño de la misma. Esta norma, es utilizada para asegurar a las partes interesadas que la compañía está certificada y que puede cumplir con los requisitos internos, legales en función del país y el escenario, y del cliente.

Esta norma, proporciona a las compañías un entorno confiable que les permita continuar ofreciendo sus servicios incluso bajo

circunstancias adversas, protegiendo a sus trabajadores, manteniendo su imagen de marca y proporcionando la capacidad de seguir operando.

Dentro de dichas normas, se ha abordado el método de resolución del problema inicial, de forma que nos permita la resolución de cualquier contingencia en del departamento CC24h, con cualquiera de los servicios que dicho departamento requiere para su funcionamiento. El problema se ha abordado desde el punto de vista del negocio, no desde el punto de vista exclusivamente de IT. De esta forma tenemos una visión más global, implicamos a todo el personal requerido independientemente del departamento en el que trabaje y conseguimos integrar el plan en el modelo de negocio.

5.1.1 Política de continuidad de negocio

En primer lugar entrando ya en lo que sería el método de resolución y siguiendo los estándares especificados, es necesario definir una política de continuidad de negocio. Se debe especificar el alcance y el gobierno del plan, asignar recursos y responsabilidad, además de recoger las razones por las que se ha implementado dicho plan.

Con respecto al alcance, se ha definido la implementación del plan de contingencia del departamento CC24h, de los servicios ofrecidos por dicho departamento.

Como recursos, se asigna un jefe de proyecto, un responsable del plan y el tiempo necesario de la jornada de los técnicos y operadores que se requiera. En cuanto a recursos materiales se asigna una sala de proyecto, con todo el material informático y de oficina necesario.

Con respecto a las responsabilidades, el jefe de proyecto será responsable durante el desarrollo del proyecto, y posteriormente la responsabilidad recaerá en la figura del responsable del plan. La responsable del departamento CC24h es responsable de que toda la información requerida para la realización del proyecto sea proporcionada al jefe de proyecto.

En cuanto a las razones por las que se decide comenzar la implementación del plan, hay varias. La más importante es el imperativo legal, que obliga a realizar rescates en un tiempo determinado, en función de la normativa en cada comunidad autónoma. En segundo lugar, se trata de un requisito de los clientes, muchos de los cuales demandan un servicio de mantenimiento de 24 horas. En tercer lugar, se percibe un riesgo alto en la imagen de marca, que podría provocar pérdida de clientes si no se es capaz de proporcionar el servicio con la calidad requerida y dentro de los tiempos asumidos en los contratos.

El documento “Política de continuidad de negocio” se encuentra en el anexo E de este proyecto.

5.1.2 Desarrollo del plan de continuidad de negocio

Una vez definida la política de continuidad de negocio, se comienza con las distintas fases del proceso, tal y como indican las normas ISO 22301 y UNE 71599, y que son las siguientes:

- Conocer la compañía e identificar los procesos críticos. En dicha fase se deberá realizar el análisis de riesgos y el análisis de impacto sobre el negocio.
- Definición de la estrategia de continuidad de negocio. Consiste en desarrollar alternativas a adoptar en cada uno de los aspectos que tenemos bajo control, cuando ocurra alguna incidencia o desastre.
- Desarrollo e implantación del plan de continuidad del negocio, en función de los resultados obtenidos en las dos fases previas.
- Prueba, mantenimiento y revisión del plan.
- Introducción del plan en la cultura de la organización, concienciando e implicando a todos los actores necesarios.

En la siguiente imagen puede verse de forma gráfica el proceso para desarrollar el plan de continuidad de negocio

Figura 13

Para ello, iremos entrando en más detalle en cada una de las fases en los siguientes apartados

5.1.2.1 Entendimiento de la organización

En primer lugar, resulta necesario acometer una fase de comprensión de la compañía e identificación de cuáles son los procesos más críticos. En el caso que nos ocupa, no es necesario ampliarlo a toda la organización, puesto que el plan abordará solamente un departamento considerado estratégico por la dirección, el departamento CC24h.

Por ello, se comenzará realizando el análisis de impacto, y posteriormente se realizará el análisis de riesgos

- **Análisis de impacto**

El análisis de impacto se inicia con un inventario de los procesos críticos del departamento CC24h, especificando además los tiempos de recuperación de los mismos antes de sufrir pérdidas graves.

En primer lugar se identifican los procesos con la frecuencia en que son realizados por personal del departamento.

Proceso	Descripción	Frecuencia
Rescate	Una o varias personas están atrapadas en un ascensor y hay que rescatarlas en un tiempo máximo	Semanal
Incidencia telefónica	Un usuario abre una incidencia en un aparato elevador y hay que solucionarla	Diaria
Incidencia Telealarma	El sistema de telealarma detecta una avería o futura avería en un aparato elevador y hay que resolverla	Diaria
Mantenimiento	Por medio de una telealarma llega la solicitud de mantenimiento de un aparato elevador	Diaria

Tabla 8

Una vez identificados dichos procesos, se procede a describir los componentes de cada uno de ellos. Es necesario especificar tanto los componentes software, como el hardware para cada uno de ellos.

Con respecto a los componentes software deberemos detallar su nombre, una breve descripción, la criticidad del sistema de 0 a 10 (siendo 10 criticidad máxima), cuantos clientes utilizan dicho sistema y quién es la persona responsable de dicho servicio

Para los componentes hardware recogeremos el tipo, una descripción breve con los detalles del modelo y configuración, el proveedor, la criticidad y la ubicación física del mismo.

Y por último, para las comunicaciones detallaremos la descripción de la línea, el tipo, la criticidad y la localización física.

- Proceso rescate
    - Sistemas

Nombre	Descripción	Criticidad	Clientes	Responsble
CAT	Centro atención telefónica	10	23	Departamento IT
Mensajes a móviles	Aplicación para el envío de SMS	8	2160	CC24h/ Departamento de IT
Datos departamentales	Datos administrativos CC24h	6	23	Departamento de IT
Correo electrónico	Sistema de envío/recepción de emails	6	2160	Departamento de IT

Tabla 9

    - Hardware

Tipo hardware	Detalles / Configuración	Proveedor	Localización	Criticidad
Servidores CAT	Cluster 2 nodos HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM, SAN fibber channel	HP	CPD Principal	10
Antenas mensajes a móviles	Antenas usb con tarjeta sim para envío de mensajes	Movistar	CPD principal	9
Almacenamiento	Cabina almacenamiento NAS	Netapp	CPD principal	10
Servidor email	HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM	HP	CPD Principal	7
Teléfono móvil	Samsung Galaxy Pocket	Samsung	Móvil, donde esté el	10

			técnico	
PC's operadores	HP Compaq pro 4300	HP	Oficina principal	9

Tabla 10

- Comunicaciones

Descripción	Tipo	Localización	Criticidad
Acceso a Internet	MPSL	CPD principal	7
Líneas telefonía	Móvil para el técnico / fijas para el envío mensajes sms	Diferentes ubicaciones / CPD Central	10

Tabla 11

- Proceso incidencia telefónica
  - Sistemas

Nombre	Descripción	Criticidad	Clientes	Responsable
CAT	Centro atención telefónica	10	23	Departamento IT
Mensajes a móviles	Aplicación para el envío de SMS	8	2160	CC24h/ Departamento de IT
Datos departamentales	Datos administrativos CC24h	6	23	Departamento de IT
Correo electrónico	Sistema de envío/recepción de emails	6	2160	Departamento de IT

Tabla 12

  - Hardware

Tipo hardware	Detalles / Configuración	Proveedor	Localización	Criticidad
Servidores CAT	Cluster 2 nodos HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM, SAN fibber channel	HP	CPD Principal	10
Antenas	Antenas usb con	Movistar	CPD principal	9

mensajes a móviles	tarjeta sim para envío de mensajes			
Almacenamiento	Cabina almacenamiento NAS	Netapp	CPD principal	10
Servidor email	HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM	HP	CPD Principal	7
Teléfono móvil	Samsung Galaxy Pocket	Samsung	Móvil, donde esté el técnico	10
PC's operadores	HP Compaq pro 4300	HP	Oficina principal	9
Fax	Philips PPF631E Fax	Philips	Oficina principal	4

Tabla 13

- Comunicaciones

Descripción	Tipo	Localización	Criticidad
Acceso a Internet	MPSL	CPD principal	7
Líneas telefonía	Móvil para el técnico / fijas para el envío mensajes sms	Diferentes ubicaciones / CPD Central	10
Línea fax	Analógica	CPD Central	4

Tabla 14

- Proceso Incidencia Telealarma
  - Sistemas

Nombre	Descripción	Criticidad	Clientes	Responsable
Telealarmas	Sistema aparatos con telealarma	7	5432	CC24h/ Departamento de IT
EAR	Sistema aparatos con EAR	9	86543	CC24h/ Departamento de IT
Dielro	Sistema aparatos con Dielro	8	23456	CC24h/ Departamento de IT
Escaleras	Sistema de	9	17456	CC24h/

	envío/recepción de emails			Departamento de IT
CAT	Centro atención telefónica	10	23	Departamento IT
Mensajes a móviles	Aplicación para el envío de SMS	8	2160	CC24h/ Departamento de IT
Datos departamentales	Datos administrativos CC24h	6	23	Departamento de IT

Tabla 15

- Hardware

Tipo hardware	Detalles / Configuración	Proveedor	Localización	Criticidad
Servidor telealarmas	HP DL380 2 procesadores Dual Core Intel Xeon, Memoria 8 GB SDRAM, 5X72Gb HD	HP	CPD Principal	6
Servidor EAR	HP DL380 4 procesadores Dual Core Intel Xeon, Memoria 16 GB SDRAM, 5X72Gb HD	HP	CPD Principal	10
Servidor Dielro	HP DL380 2 procesadores Dual Core Intel Xeon, Memoria 8 GB SDRAM, 5X72Gb HD	HP	CPD Principal	10
Servidor Escaleras	HP DL340 2 procesadores Dual Core Intel Xeon, Memoria 6 GB SDRAM, 5X72Gb HD	HP	CPD Principal	8
Modems telealarmas	Zyxel 4560	Zyxel	CPD Principal	6
Modems EAR	3Com 3c866	3Com	CPD Principal	10
Modems Dielro	Quatech PC D 101 Interface	Quatech	CPD Principal	10
Modems Escaleras	3Com 2950	3Com	CPD Principal	8
Servidores CAT	Cluster 2 nodos HP DL380	HP	CPD Principal	10

	4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM, SAN fibber channel			
Antenas mensajes a móviles	Antenas usb con tarjeta sim para envío de mensajes	Movistar	CPD principal	9
Almacenamiento	Cabina almacenamiento NAS	Netapp	CPD principal	10
Teléfono móvil	Samsung Galaxy Pocket	Samsung	Móvil, donde esté el técnico	10
PC's operadores	HP Compaq pro 4300	HP	Oficina principal	9
Fax	Philips PPF631E Fax	Philips	Oficina principal	4

Tabla 16

- Comunicaciones

Descripción	Tipo	Localización	Criticidad
Líneas telefonía móvil	Móvil para los técnicos	Diferentes ubicaciones	10
Líneas módems telealarmas	Analógica para la recepción de avisos de las telealarmas	CPD Central	10

Tabla 17

- Proceso mantenimiento (bajo demanda de telealarma automática).
    - Sistemas

Nombre	Descripción	Criticidad	Clientes	Responsable
Telealarmas	Sistema aparatos con telealarma	7	5432	CC24h/ Departamento de IT
EAR	Sistema aparatos con EAR	9	86543	CC24h/ Departamento de IT
Dielro	Sistema aparatos con Dielro	8	23456	CC24h/ Departamento de IT
Escaleras	Sistema de envío/recepción de emails	9	17456	CC24h/ Departamento de IT
CAT	Centro atención telefónica	10	23	Departamento IT
Mensajes a móviles	Aplicación para el envío de SMS	8	2160	CC24h/ Departamento de IT
Datos departamentales	Datos administrativos CC24h	6	23	Departamento de IT
Correo electrónico	Sistema de envío/recepción de emails	6	2160	Departamento de IT

Tabla 18

    - Hardware

Tipo hardware	Detalles / Configuración	Proveedor	Localización	Criticidad
Servidor telealarmas	HP DL380 2 procesadores Dual Core Intel Xeon, Memoria 8 GB SDRAM, 5X72Gb HD	HP	CPD Principal	6
Servidor EAR	HP DL380 4 procesadores Dual Core Intel Xeon, Memoria 16 GB SDRAM, 5X72Gb HD	HP	CPD Principal	10
Servidor Dielro	HP DL380 2 procesadores	HP	CPD Principal	10

	Dual Core Intel Xeon, Memoria 8 GB SDRAM, 5X72Gb HD			
Servidor Escaleras	HP DL340 2 procesadores Dual Core Intel Xeon, Memoria 6 GB SDRAM, 5X72Gb HD	HP	CPD Principal	8
Modems telealarmas	Zyxel 4560	Zyxel	CPD Principal	6
Modems EAR	3Com 3c866	3Com	CPD Principal	10
Modems Dielro	Quatech PC D 101 Interface	Quatech	CPD Principal	10
Modems Escaleras	3Com 2950	3Com	CPD Principal	8
Servidores CAT	Cluster 2 nodos HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM, SAN fibber channel	HP	CPD Principal	10
Antenas mensajes a móviles	Antenas usb con tarjeta sim para envío de mensajes	Movistar	CPD principal	9
Almacenamiento	Cabina almacenamiento NAS	Netapp	CPD principal	10
Servidor email	HP DL380 4 procesadores Quad Core Intel Xeon, Memoria 32 GB SDRAM	HP	CPD Principal	7
Teléfono móvil	Samsung Galaxy Pocket	Samsung	Móvil, donde esté el técnico	10
PC's operadores	HP Compaq pro 4300	HP	Oficina principal	9
Fax	Philips PPF631E Fax	Philips	Oficina principal	4

Tabla 19

- Comunicaciones

Descripción	Tipo	Localización	Criticidad
Líneas telefonía móvil	Móvil para el técnico	Diferentes ubicaciones	10
Líneas módems telealarmas	Analógica para la recepción de las llamadas de los aparatos	CPD Central	10
Acceso a Internet	MPSL	CPD principal	7

Tabla 20

- Tiempos máximos de recuperación de los procesos

Los tiempos máximos para cada uno de los procesos han sido obtenidos por medio de entrevistas presenciales a personal del departamento CC24H. Dicho personal es el que mejor conoce todos estos procesos, y tiene una mejor aproximación a lo que el negocio requiere de su área.

Al igual que en el punto anterior, la criticidad se evalua de 1 a 10, siendo 10 criticidad máxima.

Rescate

Proceso	Criticidad	Tiempo máximo interrupción
Rescate	10	15 minutos

Tabla 21

El proceso de rescate de una persona o personas atrapadas en un aparato elevador es el proceso más crítico de todos los incluidos en este plan de contingencia. Es por ello que su criticidad es máxima y no es admisible que este proceso no esté operativo más de 15 minutos. Ello es debido a los tiempos máximos de rescate, que en algunas comunidades autónomas pueden ser de solo una hora.

Indidencia telefónica

Proceso	Criticidad	Tiempo máximo interrupción
Incidencia Telefónica	9	1 hora

Tabla 22

El proceso de atención de una incidencia telefónica es también un proceso crítico. El que un cliente llame al teléfono de atención telefónica y no reciba inmediata respuesta, no tiene un coste directo, pero si indirecto, y sobre todo, de daño a la imagen de marca. No es tan crítico como pudiera ser un rescate, porque su no cumplimiento no tiene responsabilidades penales.

Incidencia Telealarma

Proceso	Criticidad	Tiempo máximo interrupción
Incidencia Telealarma	6	1 día

Tabla 23

Con respecto al proceso de atención de una incidencia generada por la telealarma de un aparato elevador, podemos permitir unos márgenes más amplios. La criticidad no es alta, puesto que la incidencia nos llegará por medio de teléfono, cuando algún usuario la detecte. Lo mismo sucede con el tiempo máximo de interrupción del proceso, que se permite que sea de un día, puesto que su criticidad no es máxima. En este caso lo único que perdemos al no disponer de este proceso es que la incidencia se detecte automáticamente y pueda resolverse sin que el cliente se dé cuenta. Es por tanto un proceso importante, pero no crítico

Mantenimiento

Proceso	Criticidad	Tiempo máximo interrupción
Mantenimiento	4	1 día

Tabla 24

El proceso de mantenimiento es el menos crítico de los analizados. Los mantenimientos de los aparatos se realizan con una frecuencia mensual. En este caso el proceso informa de que hay que realizar el mantenimiento en un determinado aparato, pero como cada técnico recibe a principios de mes el listado de los que debe mantener, es posible prescindir de este proceso durante un día sin que se produzca ningún perjuicio.

IDENTIFICACIÓN Y ANALISIS DE RIESGOS

A continuación se procederá a realizar la identificación y el análisis de riesgos, donde se tratara de realizar una identificación clara de los mismos, para posteriormente poder gestionarlos y tratar de reducir su impacto sobre el negocio.

Utilizando el inventario de procesos que hemos realizado, se procede a la elaboración del inventario de activos con su correspondiente valor para el negocio, con el objetivo de conocer el riesgo que implica

Activo	Categoría	Ubicación	Valor
Servidores CAT	Hardware	CPD	Alto
Servidor email	Hardware	CPD	Medio
Servidor EAR	Hardware	CPD	Alto
Servidor Dielro	Hardware	CPD	Alto
Servidor Telealarmas	Hardware	CPD	Bajo
Servidor escaleras	Hardware	CPD	Medio
Modem Telealarmas	Hardware	CPD	Bajo
Modem EAR	Hardware	CPD	Alto
Modem Dielro	Hardware	CPD	Alto
Modem Escaleras	Hardware	CPD	Alto

Antenas mensajes móviles	Hardware	CPD	Alto
Almacenamiento	Hardware	CPD	Alto
Teléfono móvil	Comunicaciones	Diversas ubicaciones	Alto
PC's Operadores	Hardware	Departamento cc24h	Alto
Fax	Hardware	Departamento cc24h	Bajo
Líneas telefonía	Comunicaciones	CPD	Alto
Software telealarmas	Software	CPD	Alto
Software EAR	Software	CPD	Alto
Software Dielro	Software	CPD	Alto
Software escaleras	Software	CPD	Alto
Aplicación CAT	Software	CPD	Alto
Aplicación mensajes a móviles	Software	CPD	Alto
Datos departamentales	Software	CPD	Medio
Email	Software	CPD	Medio
Acceso a Internet	Comunicaciones	CPD	Medio

Tabla 25

5.1.2.2 Definición de la estrategia de continuidad de negocio.

Para la definición de la estrategia más adecuada con respecto a la continuidad del negocio, es importante tener en cuenta los tres factores más relevantes, y que son los que se muestra en el siguiente gráfico.

Figura 14

En primer lugar, debemos contemplar la alta disponibilidad del sistema, es decir, debemos asegurar que el sistema esté operativo durante todo el tiempo. Entendiendo que habrá tiempos de parada para actualizaciones de seguridad, actualizaciones de software, cambios en el hardware.

De forma simultánea debemos ser capaces de garantizar la protección de los datos alojados en el sistema. Nos dotaremos de las medidas necesarias para garantizar su integridad y confidencialidad, cumpliendo siempre la normativa legal que aplique a los mismos, como por ejemplo la LOPD (Ley Orgánica de protección de datos).

Y por último, dispondremos del plan de recuperación de desastres, fundamental para la continuidad del negocio en caso de una contingencia.

5.1.2.3 Desarrollo e implantación del plan.

Una vez que disponemos de suficiente conocimiento de los procesos de la compañía en cuanto al departamento CC24h y hemos valorado los riesgos que pueden afectarles, además de decidir cuál es la estrategia de continuidad más adecuada para el negocio, podemos proceder a desarrollar e implantar el plan de contingencia.

Para ello, debemos definir los procedimientos de aviso y actuación ante desastres o incidencias que pueda provocar el lanzamiento del plan. Además, definiremos las personas y equipos necesarios para el desarrollo del plan, así como las funciones y responsabilidades de cada uno de ellos, junto con las dependencias por las que se relacionan. Y por último, generaremos los procedimientos de actuación ante desastres, así como la estrategia de vuelta a la normalidad.

5.1.2.3.1 Grupos de trabajo

Definimos en este apartado los distintos equipos de trabajo que serán necesarios para la puesta en marcha y ejecución del plan. Cada uno de los equipos tendrá unas funciones, unas responsabilidades y procedimientos a seguir en función del tipo de incidencia que suceda. Es importante señalar que el número de miembros de los equipos podrá variar en función de las necesidades y que aunque se denominen equipos, algunos pueden estar formados solamente por una persona.

Los grupos propuestos son los siguientes:

- Usuarios clave: grupo de usuarios del sistema que pueden realizar pruebas y garantizar que los diferentes servicios funcionan adecuadamente. Estará formado que por personas que conocen las aplicaciones y que deberán definir previamente las pruebas a realizar en los sistemas. En este caso se considera usuarios clave a las personas que trabajan en el departamento CC24h.

- Equipo de recuperación: su función es restaurar los sistemas necesarios para que el departamento CC24h pueda trabajar con normalidad. Para ello deberá operar la infraestructura y será responsable de todos los sistemas: ordenadores, servidores, comunicaciones de datos, de voz,… En este equipo se incluyen los ingenieros de cada una de las áreas definidos en el punto 2.3.2 y que son los siguientes ingeniero de hardware, ingeniero de sistemas, ingeniero de telecomunicaciones, ingeniero de aplicaciones y responsable de comunicaciones
- Equipo de comunicación: será el encargado de gestionar las comunicaciones con los clientes y prensa si fuera necesario. Su función consiste en proporcionar la información al exterior desde un solo punto para evitar mensajes inconsistentes. Sus principales funciones serán: comunicación con los clientes y relación con la prensa. Esté equipo estará en constante comunicación con el equipo de recuperación y con el comité de contingencias para disponer siempre de la información actualizada y veraz con respecto a la situación
- Comité de contingencias: es el grupo responsable del éxito de plan y que deberá tomar las decisiones que sean necesarias. Su objetivo es minimizar el riesgo y la incertidumbre durante la puesta en marcha del plan de contingencia. El responsable del plan será miembro de este comité, que deberá estar en permanente contacto tanto con el equipo de recuperación como del de comunicación. Sus funciones básicas serán: activar o no el plan de contingencia, analizar la situación para tomar decisiones, iniciar las notificaciones que sean necesarias y realizar un seguimiento del plan para verificar que se completa con éxito.

5.1.2.3.2 Procedimientos

Cuando ya hemos finalizado la tarea de definir los equipos de trabajo, las responsabilidades de cada uno de ellos y las interrelaciones entre ellos, debemos definir los procedimientos que se seguirán durante el desarrollo del plan.

Para la estructuración de los procedimientos, se definen cuatro fases durante la ejecución del plan: fase de alerta, fase de transición, fase de recuperación y fase de vuelta a la normalidad. A continuación se detalla cada una de las fases con sus procedimientos.

- **Fase de alerta**

En esta fase se definen los procedimientos de actuación en las primeras etapas de una contingencia. A su vez, se divide en tres fases:

- Notificación: procedimiento en el que se detalla la como debe realizarse la notificación y a que personas.
- Evaluación: consiste en la evaluación de la situación y en una primera valoración del alcance de la contingencia. En función de ello, se definirán las estrategias.

- Lanzamiento del plan: el responsable del plan decidirá si se inicia o no el plan, en función del alcance de los daños

A continuación se detalla cada una de las partes:

NOTIFICACIÓN

Para la notificación de un incidente, suponemos que siempre nos llegará la información a través del CAU. Podría ser posible que alguna persona de la empresa, o más concretamente del CC24h avisará directamente al responsable del plan, pero en cualquier caso, el responsable deberá informar al CAU para arrancar el procedimiento. Además parece conveniente centralizar la información en un solo lugar, y el más adecuado es el CAU que está operativo 24 horas.

Por tanto la notificación deberá realizarse de acuerdo a la siguiente tabla:

FASE	EVENTO	ACCIÓN
1	Contingencia/Incidencia detectada por personal de CC24h	Apertura de incidencia en el CAU de IT
2	El CAU tiene conocimiento de que ha sucedido algo en el departamento 24h	El CAU informa al responsable del plan. En caso necesario, el CAU informa a los equipos implicados en el plan.

Tabla 26

EVALUACIÓN

Cuando el responsable del plan ya ha sido informado del incidente, procederá a analizar la información disponible para evaluar la situación. Para ello, necesitará la información más detallada posible, por lo que se deberá realizar previamente una formación al personal del CAU sobre este asunto.

Además, el responsable deberá informar a los distintos grupos de trabajo de la incidencia ocurrida y de la situación actual. De esta manera dichos equipos están avisados y a la espera de que se decida arrancar o no el plan.

FASE	EVENTO	ACCIÓN
3	El responsable del plan es informado de la incidencia ocurrida	El responsable del plan evaluará la situación. En función de dicha situación deberá decidir si activar o no el plan de contingencia Deberá informar a los responsables de los siguientes equipos de trabajo:

		• Comité de dirección • Equipo de recuperación • Equipo de comunicación • Usuarios clave.

Tabla 27

LANZAMIENTO DEL PLAN

Cuando el responsable del plan decide poner en marcha el plan de contingencia, debe iniciarse desde el CAU la comunicación de la decisión a los diferentes equipos de trabajo, para poder arrancar los procedimientos de actuación de cada uno de ellos. Se deberá informar también a la dirección de la empresa.

FASE	EVENTO	ACCIÓN
4	El responsable del plan toma la decisión de activar el plan de contingencia	• Se informa a los distintos equipos de trabajo • Se informa a la dirección de la empresa
5	Se da por finalizada la fase de alerta y se pasa a la fase de transición.	

Tabla 28

- Fase de transición

La fase de transición es la que transcurre entre el momento en el que se arranca el plan y el comienzo de la fase en la que se realiza la recuperación del sistema o sistemas. Es una fase de preparación de lo que posteriormente será la recuperación y que es muy importante para garantizar que los tiempos establecidos se puedan cumplir

En ella es fundamental que el responsable del plan sea capaz de coordinar a los diferentes equipos para comenzar a trabajar a la mayor brevedad posible

Dentro de esta fase, definimos dos procedimientos fundamentales:

- Procedimiento de reunión y gestión logística

  En este procedimiento y en función de la estrategia definida de respaldo, que en este caso consiste en utilizar un CPD de Backup, se define el punto de reunión para el personal que deberá trabajar en la recuperación y la gestión de la logística necesaria para poder mantener el servicio desde dicho CPD.

  Una vez lanzado el plan e informados los correspondientes equipos, deberán desplazarse al centro de reunión. En el caso de incidencia parcial, el centro de reunión será la oficina principal del departamento CC24h y en el caso de incidencia total, será el CPD de respaldo.

Desde el CAU se informará a los operadores del CC24h que se incorporen a su puesto de trabajo con posterioridad al arranque del plan, de que deberán hacerlo en el centro de respaldo (solo en el caso de incidencia total). También en este caso, el responsable de comunicaciones informa al operador de que debe arrancar su plan de contingencia, desviando los teléfonos al CPD de respaldo, puesto que los servicios van a comenzar a proporcionarse desde allí.

También en este mismo caso de incidencia total, el responsable del plan deberá contactar con el equipo de recuperación, para que los ingenieros comiencen a trabajar en el plan, trasladándose al CPD de respaldo.

- Procedimiento de puesta en marcha del CPD de respaldo.

Una vez que disponemos de todos los recursos humanos en el CPD de respaldo, debemos establecer el procedimiento necesario para arrancar los servicios desde dichas instalaciones.

El procedimiento arranca cuando el responsable del plan se pone en contacto con los responsables de todas las áreas (ingeniero de hardware, ingeniero de aplicaciones, ingeniero de sistemas y responsable de comunicaciones) y les informa de que se ha producido una incidencia que afecta a la totalidad del sistema y es necesario comenzar a proporcionar el servicio desde el centro de respaldo.

Seguidamente, el responsable del plan contacta con el responsable del departamento CC24h, para informarle de que los operadores deben acudir o trasladarse a la oficina que se encuentras junto al CPD de respaldo, puesto que ha ocurrido una incidencia.

El siguiente paso consiste en que el responsable de comunicaciones informe al operador de comunicaciones de la incidencia, y que el operador arranque su plan de contingencia. Inmediatamente desvía el número de atención telefónica ante averías en equipos elevadores a la centralita del CPD de respaldo. Se solicita asimismo el desvío del número de fax al número de la oficina del CPD de respaldo y el desvío de las llamadas de las telealarmas también a números de dicho CPD. El operador comprueba también que la centralita del CPD de respaldo se encuentra correctamente operativa y plenamente funcional para dar el servicio.

En paralelo:

- el ingeniero de sistemas revisa el funcionamiento del sistema de correo electrónico, del servidor de aplicaciones y de la base de datos. Asimismo, verifica que los datos están sincronizados correctamente al instante posterior al suceso de la incidencia en el CPD principal
- el ingeniero de hardware y microinformática comprueba que el servidor se encuentra en un estado óptimo y realiza pruebas con los pc's de los operadores para comprobar que tienen

correctamente configurado el acceso al correo electrónico y al resto de aplicaciones.

- el ingeniero de aplicaciones confirma que tanto el CAT, como los mensajes a móviles como el resto de aplicaciones están funcionando correctamente en el CPD de respaldo.

Una vez finalizadas las tareas de las distintas áreas, un operador del CC24h comprueba el acceso a todos los sistemas de forma secuencial. En primer lugar verifica el funcionamiento del CAT, comprobando que los datos son correctos, para a continuación realizar pruebas de correo electrónico, acceso a Internet…. Cuando ha finalizado, confirma al responsable del departamento CC24h que todos los servicios están operativos.

El responsable del departamento CC24h confirma que todos los servicios están operativos, y que el departamento está funcionando adecuadamente, teniendo en cuenta las restricciones de que el centro de respaldo dispone de menores recursos en comparación con el principal y el rendimiento que ofrece es menor.

- Fase de recuperación

En el supuesto de avería total del sistema, la fase de recuperación se realiza en el punto anterior, puesto que la propia puesta en marcha del CPD de respaldo ya supone la recuperación del sistema.

En el caso de avería parcial, y solamente sea necesario recuperar una parte del sistema, es necesario definir los procedimientos de la fase de recuperación para dicho subsistema.

Esta fase a su vez, se divide en dos: procedimientos de restauración y procedimientos de gestión y soporte.

  - Procedimiento de restauración

    En este procedimiento se detallan los pasos a seguir para la restauración de cualquiera de los subsistemas incluidos en el plan de contingencia:

    1. Tras detectarse la incidencia e informarse al CAU, se contacta con el responsable del plan
    2. El responsable del plan verifica que tipo de incidencia parcial es la que se ha producido y contacta con el responsable del área correspondiente (hardware, sistemas, aplicaciones o telecomunicaciones)
    3. El responsable del área realiza el análisis en profundidad de la incidencia, y verifica si puede resolverla. En el caso de que pueda resolverla por sus propios medios, lo hace, informa al responsable del plan y el procedimiento continúa en el paso 5.
    4. En el caso de que el responsable no pueda resolver la incidencia, contacta con el correspondiente

soporte técnico, que es quien procede a resolverla y una vez resuelta, el responsable del área contacta con el responsable del plan para confirmarle que la incidencia ha sido solucionada.

5. El responsable del plan se pone en contacto con el CAU, e indica que la incidencia ha sido resuelta y que se puede trabajar con normalidad.
6. El CAU registra la información de resolución de la incidencia y pasa la incidencia al estado “pendiente de confirmación”
7. El CAU contacta con el usuario o técnico que abrió la incidencia y le indica que ha sido solucionada.

- Procedimiento de gestión y soporte.

Una vez restaurado el sistema en su totalidad, es necesario verificar el correcto funcionamiento del mismo y realizar el mantenimiento necesario. Con respecto a la comprobación y verificación del correcto funcionamiento de los sistemas, los operadores del CC24h serán las personas responsables.

El procedimiento dispondría de los siguientes pasos:

1. El CAU contacta con algunos de los operadores del CC24h que estén disponibles en ese momento y les indica que comiencen las pruebas del sistema. En el caso de avería parcial solo se deberá revisar el subsistema afectado y en el caso de avería total, deberá seguir
2. Cuando el CAU recibe confirmación por parte del usuario o técnico de que puede trabajar con normalidad, o bien cuando han pasado más de 8 horas desde que se le informó, la incidencia pasa a estado “solucionada”
3. Cuando pasan 72 horas sin recibir ningún tipo de reclamación sobre la incidencia, el estado de la misma se pasa a cerrada y se da por finalizado el procedimiento.
4. En paralelo a los puntos 2 y 3, los responsables de cada una de las áreas o todos en el caso de incidencia total, revisan el sistema para comprobar que todos los subsistemas sobre los que tienen responsabilidad, están funcionando

- Fase de vuelta al estado normal

Cuando ya hemos conseguido restaurar el servicio y hemos resuelto la contingencia, es el momento de decidir las estrategias y acciones necesarias para recuperar el funcionamiento normal de todos los servicios. En esta fase se incluye tanto un análisis de impacto en el que tenemos que valorar los equipos e infraestructuras dañadas, como una segunda fase de vuelta al estado normal, que incluye los mecanismos de comprar de nuevos equipos, reparación de infraestructuras,…..

- Análisis de impacto

Dentro de la vuelta al estado normal, es necesario realizar un análisis del impacto que ha provocado la incidencia en las infraestructuras del sistema.

En el caso de incidencia total que afecta a todo el sistema y que además requiere traslado del servicio al CPD de respaldo, el procedimiento consiste en acceder al CPD principal y realizar un inventario de los activos afectados. Esta tarea será realizada por el responsable del plan junto con el responsable del CC24h.

Para ello, se utilizará la siguiente tabla

ACTIVO	ID	ESTADO	VALOR ESTIMADO
Servidor	4589789JTD	Destruido	3000€
Rack	AW478956	Reparable	1500€
Mesa	458796	No afectado	Amortizado

Tabla 29

En activo introduciremos el tipo de objeto que ha sido afectado por la incidencia, que puede ser un servidor, un switch, un teléfono, el dispositivo de fax,…

En ID introduciremos un dato que nos permita identificar el activo en concreto. En el caso de dispositivos electrónicos utilizaremos el número de serie. En el caso de otro tipo de activos como mesas o sillas que no dispongan de dicha referencia, utilizaremos el número con el que son registrados en el inventario.

En el estado tendremos tres opciones posibles:

1. Destruido: el activo ha quedado inutilizable, no se puede reparar y debe ser reemplazado por uno nuevo.
2. Reparable: el activo ha sufrido daños, pero se puede reparar, no es necesario acometer una compra de uno nuevo.
3. No afectado: la incidencia no ha afectado al activo.

En el campo valor estimado, debemos reflejar el valor que consideramos que podría tener el activo. En el caso de que ya haya sido amortizado, también podemos reflejarlo.

Para el caso de incidencia parcial, el procedimiento es el mismo. El responsable del plan acompañado del responsable del CC24h visitara el CPD principal y la oficina para revisar cuales han sido

los daños y elaborar el inventario siguiendo el mismo formato de la tabla anterior.

- Procedimientos vuelta a la normalidad.

Una vez que hemos sido capaces de determinar el impacto que la incidencia ha tenido en nuestra infraestructura, debemos contemplar las acciones necesarias para restablecerla al estado inicial, que entendemos que es el estado óptimo de la misma.

Para ello, contaremos con la tabla de análisis de impacto elaborada en el punto anterior, que nos indica que componentes de la infraestructura hay que comprar nuevos, cuales pueden repararse y cuales pueden continuar porque no han resultado dañados con la incidencia.

Utilizando dicha tabla, elaboraremos una nueva en la que especificaremos el activo a comprar, el proveedor, el precio estimado y el plazo de entrega, tal y como se muestra a continuación:

ACTIVO	Proveedor	Importe estimado	Plazo entrega
Servidor	HP	9000€	30 días
Switch	Cisco	3000€	45 días
Mesa	Muebles Martín	300	20 días

Tabla 30

5.1.2.4 Pruebas, mantenimiento y revisión del plan.

Cuando ya tenemos definido el plan, en primer lugar tenemos que acometer un plan de pruebas que asegure que el plan proporciona soluciones a los problemas que se planteaban en la fase de análisis.

Seguidamente, deberemos organizar el mantenimiento, puesto que un plan que no se mantiene, tiende a quedarse obsoleto en un breve tiempo. El plan de mantenimiento deberá recoger todas las medidas correctivas sobre el plan, que permitan su evolución en función de cómo vayan cambiando las circunstancias que lo afectan.

Y finalmente, deberemos realizar una revisión completa del plan, que incluya tanto el propio plan, como el plan de pruebas y el plan de mantenimiento.

5.1.2.4.1 Plan de Pruebas

Tal y como comentábamos en el punto anterior, una vez completado el plan de contingencia, debe ser probado para verificar que es capaz de mantener la continuidad en los servicios críticos para el CC24h. Es importante realizar pruebas, puesto que debemos encontrar posibles problemas que no hayamos tenido en cuenta durante el desarrollo del plan.

Los principales objetivos con los que acometemos el plan de pruebas son los siguientes:

- Identificar mejoras en el desarrollo y ejecución del plan
- Concienciación de la importancia del plan y formación para los equipos humanos implicados.
- Verificación de los tiempos de respuesta y de la efectividad del plan, confirmando que está alineados con el diseño realizado
- Comprobación de que los procedimientos resuelven los problemas planteados y aplicación de mejoras a los mismos
- Evaluación de forma detalla de los costes de las operaciones a realizar en caso de contingencia.

En primer lugar, procedemos a definir la tabla de pruebas a realizar

Prueba	Descripción	Responsable
1	Avería en telealarmas Dielro	Operador.
2	Incidencia en el correo electrónico	Operador.
3	Incidencia en el sistema CAT	Operador.
4	Fallo en las antenas de envío de mensajes a móviles	Operador.
5	Desaparición o borrado accidental de los datos del departamento CC24h	Operador.
6	Fallo en la cabina de almacenamiento	Ingeniero de hardware
7	Fallo en el equipo de un operador	Ingeniero de hardware
8	Incidencia en el acceso a Internet	Operador
9	Fallo en el sistema de fax.	Operador
10	Simulación de incendio en el CPD	Responsable del plan.

Tabla 31

Una vez definidas las pruebas, cada responsable debe completarlas e informar al responsable del plan de su resultado de las mismas, tal y como se especifica en las tablas siguientes.

Prueba	Proceso	Incidencias	Resultado
1	1. Se detecta avería en el sistema Dielro, no se puede acceder a la información del servidor 2. El operador abre incidencia en el CAU, indicando que no tiene acceso a la aplicación de consulta de Dielro 3. El CAU pasa la	El CAU no	Finalizada con éxito. Insistir en la necesidad de que el CAU realice comprobaciones técnicas o solicite más

	incidencia al ingeniero de hardware 4. El ingeniero de hardware comprueba que no es un problema del servidor, sino de la aplicación y devuelve la incidencia al CAU 5. El CAU la asigna al ingeniero de sistemas que comprueba que la aplicación que gestiona los módems no está funcionado. 6. El ingeniero resuelve la incidencia e informa al CAU 7. El CAU informa al operador de que la incidencia ha sido resuelta	realiza comprobaciones de la incidencia, por lo que la asigna incorrectamente	detalles en la apertura de incidencia.
2	1. Se detecta incidencia en el correo electrónico, no se puede enviar ni recibir, el cliente no conecta 2. El operador abre incidencia en el CAU, indicando que no tiene acceso al correo electrónico 3. El CAU contacta con el ingeniero de sistemas facilitándole la información de que dispone 4. El ingeniero de sistemas revisa el sistema de correo electrónico y comprueba que el servicio que habilita el acceso rpc al buzón está detenido. 5. El ing. de sistemas contacta con el soporte técnico del fabricante, Microsoft, y abre un caso de soporte 6. El soporte técnico contacta con el ing. y le		Finalizada con éxito.

	indica cómo proceder para resolver la incidencia. 7. El ingeniero resuelve la incidencia e informa al CAU 8. El CAU informa al operador de que la incidencia ha sido resuelta		
3	1. Un operador abre incidencia en el CAU porque no puede acceder a los datos del parque de ascensores, aunque la aplicación CAT si le funciona 2. El CAU contacta con el ingeniero de aplicaciones facilitándole la información de que dispone 3. El ing. de aplicaciones revisa el CAT y comprueba que hay un problema con la BBDD. 4. El ing. de aplicaciones resuelve la incidencia e informa al CAU. 5. El CAU informa al operador de que la incidencia ha sido resuelta		Finalizada con éxito.
4	Fallo en las antenas de envío de mensajes a móviles 1. Un técnico de mantenimiento abre incidencia en el CAU porque no le están llegando los avisos por sms 2. El CAU pasa la incidencia al ing. de telecomunicaciones 3. El ing. de telecomunicaciones revisa el sistema y comprueba que las antenas están correctamente configuradas 4. El ing. de telecomunicaciones contacta con el operador y abre una incidencia		Finalizada con éxito.

	5. El operador indica que ha tenido problemas con ciertas antenas de su red, y que acaba de solucionarlo. 6. El ing. de telecom. realiza pruebas y comprueba que ya se están enviando los SMS. Devuelve la incidencia al CAU. 7. El CAU contacta con el técnico de mante. que confirma que ya recibe SMS de avisos. 8. El CAU cierra la incidencia.		
5	Desaparición o borrado accidental de los datos del departamento CC24h 1. Un operador intenta acceder al fichero de técnicos de guardia una delegación y no los encuentra en su ubicación habitual, está vacía 2. Abre incidencia en el CAU, describiendo el problema 3. El CAU lo asigna al ing. de sistemas que se conecta al servidor y no encuentra ningún problema, más allá de que los datos no se encuentran donde deberían. Lo devuelve al CAU indicando que lo pasen al personal de backup 4. El CAU lo asigna al equipo de backup 5. El equipo se pone en contacto con el usuario y concreta los datos a restaurar del backup 6. Le restauran los datos y los devuelven la incidencia al CAU para que informe al operador 7. El CAU llama al operador para que confirme que ya tiene acceso a los datos.	Valorar la posibilidad de contar dentro del plan con un ingeniero de backup y almacenamiento, para descargar de trabajo al ing. de sistemas.	Finalizada con éxito.
6	Fallo en la cabina de almacenamiento 1. Un operador abre incidencia en el CAU		Finalizada con éxito.

	porque no puede acceder al recurso datos del CC24h. Indica que le aparece el error: “no se pudo conectar la unidad D:” 2. El CAU pasa la incidencia al técnico de sistemas, que confirma que hay un problema con la cabina de almacenamiento y que parece ser el hardware 3. El CAU asigna la incidencia al ing. de hardware que confirma que es un problema con la cabina y abre incidencia con el proveedor 4. El proveedor resuelve el problema con la cabina, debido al firmware y lo confirma al ing. de hardware 5. El ing. de hardware indica al CAU que se puede indicar al usuario que el problema está resuelto 6. El CAU contacta con el operador, quien confirma que puede acceder a los datos.	Valorar la posibilidad de contar dentro del plan con un ingeniero de backup y almacenamiento, para descargar de trabajo al ing. de sistemas y/o hardware.	
7	Fallo en el equipo de un operador. 1. Un operador abre incidencia en el CAU indicando que no puede trabajar con su equipo, no tiene acceso al CAT, ni al correo ni acceso a Internet 2. El CAU tramita la incidencia y la asigna al ing. de sistemas 3. El ing. de sistemas contacta con el operador y confirma que es un problema con la red, el	Valorar la necesidad de incluir en el plan un técnico de microinformática para reducir la carga de trabajo del ing. de sistemas.	Finalizada con éxito.

	equipo no tiene conexión 4. El ing. de sistemas comprueba la configuración de la tarjeta de red que es correcta, el parcheado del armario y todo está correcto. Cambia el cable de red del equipo y se resuelve la incidencia 5. El usuario indica al CAU que el problema ha sido resuelto y que puede proceder a cerrarla.		
8	Incidencia en el acceso a Internet 1. Un operador abre incidencia en el CAU indicando que no dispone de acceso a Internet 2. El CAU tramita la incidencia y la asigna al ing. de sistemas 3. El Ing. de sistemas revisa el proxy, router y demás dispositivos de red y encuentra que todos están funcionando correctamente, el problema es que se ha caído la línea 4. Devuelve la incidencia al CAU, indicando que la asigne al ing. de telecomunicaciones 5. El ing. de teleco. confirma que hay un problema en la línea y se pone en contacto con el proveedor de comunicaciones 6. El proveedor informa que se trata de una incidencia en uno de sus nodos de la zona y que lo resolverá en 30 minutos 7. Cuando lo soluciona, se		Finalizada con éxito.

	pone en contacto con el responsable de telecomunicaciones 8. Este contacta con el CAU e indica que se puede cerrar la incidencia y contactar con el operador.		
9	Fallo en el sistema de fax. 1. Un operador intenta enviar un fax y no consigue recibir confirmación de enviado 2. Abre incidencia en el CAU y se asigna al ingeniero de hardware 3. El ingeniero de hardware revisa el fax y comprueba que es un fallo de la fuente de alimentación 4. Contacta con el proveedor que envía un fax nuevo para reemplazar el averiado 5. El ing. de hardware lo conecta e informa al CAU 6. El CAU informa al operador de que ya tiene el fax operativo.		Finalizada con éxito.
10	Simulación de incendio en el CPD 1. Se recibe una llamada en el CAU informando de que ha habido un incendio en el CPD principal 2. El CAU informa al responsable del plan 3. El responsable cataloga la incidencia como total y arranca el procedimiento 4. Informa a los responsables de todas las áreas de que es necesario comenzar a operar desde el CPD de respaldo.		Finalizada con éxito.

	5. El responsable del plan contacta con el responsable del departamento CC24h para encargarle la coordinación con los operadores, indicándoles que deben trasladarse a la oficina aledaña al CPD de respaldo. 6. El responsable de comunicaciones informa al operador de comunicaciones de la incidencia, y el operador arranca su plan de contingencia. Se desvía el número de atención telefónica ante averías en equipos elevadores a la centralita del CPD de respaldo. Se solicita asimismo el desvío del número de fax al número de la oficina del CPD de respaldo y el desvío de las llamadas de las telealarmas también a números de dicho CPD. El operador comprueba también que la centralita del CPD de respaldo se encuentra correctamente operativa y plenamente funcional para dar el servicio. 7. En paralelo, el ingeniero de sistemas revisa el funcionamiento del sistema de correo electrónico, del servidor de aplicaciones y de la base de datos. Asimismo, verifica que los datos están sincronizados correctamente al instante posterior al suceso de la incidencia		

	en el CPD principal 8. También en paralelo, el ingeniero de hardware y microinformática comprueba que el servidor se encuentra en un estado óptimo y realiza pruebas con los pc's de los operadores para comprobar que tienen correctamente configurado el acceso al correo electrónico y al resto de aplicaciones. 9. En paralelo a las anteriores tareas, el ingeniero de aplicaciones confirma que tanto el CAT, como los mensajes a móviles como el resto de aplicaciones están funcionando correctamente en el CPD de respaldo. 10. El responsable del departamento CC24h confirma que todos los servicios están operativos, y que el departamento está funcionando adecuadamente 11. El responsable del plan se pone en contacto con el CAU para informar de que la incidencia ha sido resuelta. Con la información que le ha facilitado el responsable de área, informa de los detalles de la misma 12. El CAU registra la información de resolución de la incidencia y la pasa a estado "pendiente de confirmación"		

	13. Paso 18 – El CAU contacta con el usuario o técnico que abrió la incidencia y le indica que ha sido resuelta. Si no consigue contactarle, le envía un correo electrónico. 14. El CAU recibe confirmación del usuario de que la incidencia ha sido resuelta o trascurren más de 8 horas, la incidencia pasa a estado “solucionada” 15. Tras 72 horas sin recibir información de la incidencia, se pasa la misma a estado “cerrada”. En caso de algún problema en la misma, el usuario puede volver a abrirla.		

Tabla 32

5.1.2.4.2 Plan de mantenimiento

Una vez completado y ejecutado el plan de pruebas, es necesario elaborar un procedimiento de mantenimiento del plan. No tendría sentido acometer todos los trabajos que conlleva la elaboración del plan, y luego no disponer de un procedimiento de actualización del mismo en función de los cambios que puedan surgir en la organización o de las mejoras que se detecten en los diferentes procedimientos. Mantener el plan actualizado es vital para prevenir fallos en su aplicación. Se trata de un proceso iterativo que no tiene fecha de fin, puesto que debe evaluarse y mejorarse de forma periódica.

En primer lugar, definimos como responsable del plan de mantenimiento al responsable del plan. Dicha persona tendrá la responsabilidad de seguir las directrices definidas para garantizar la evolución del plan en función de las nuevas necesidades que pueda surgir o de los cambios que se produzcan. En importante tener en cuenta que el plan es algo vivo, susceptible de cambios en el tiempo. Y es fundamental para garantizar el funcionamiento del mismo, que todos los cambios que puedan afectar a dicho plan, se reflejen en el durante el mantenimiento que se realice.

El responsable del plan, será informado de cualquier cambio en las personas responsables de las áreas, en cualquier cambio que se realice de proveedor y de cualquier otro cambio que pueda afectar al plan. En los

procedimientos del departamento CC24h se incluirá un apartado para que cualquier cambio que pueda afectar al plan, sea comunicado al responsable.

La forma más adecuada de garantizar la correcta evolución del plan sería realizar un simulacro, para comprobar que siguiendo la actual documentación del plan, se puede garantizar la continuidad del negocio. Pero la realización del mismo es complicada por varios motivos. El principal es el económico, la dificultad de encajar en unos presupuestos tan ajustados como los que hay actualmente en las empresas, unos costes que realmente no aportan a la empresa una mejora en su negocio. Está fuera de toda discusión que un plan de contingencia que no funcione adecuadamente puede dejar el negocio sin continuidad, pero en ocasiones los directivos deciden asumir riesgos, para no incurrir en ciertos costes.
Por otro lado, está la dificultad de detener los sistemas para realizarlo. Evidentemente, el simulacro debe ser lo más real posible, y para ello hay que forzar la caída del CPD principal o bien detenerlo, y arrancar la ejecución del plan, con todos los inconvenientes que conlleva al negocio, especialmente al departamento CC24h y a su personal.

Por tanto, y dada la dificultad de verificar que se está realizando un buen mantenimiento del plan, y de que este sigue siendo válido en el estado actual, se propone la realización de una serie de acciones sencillas, que permiten verificar que las medidas del plan siguen teniendo vigencia, y que el plan está actualizado. En ningún caso dichas medidas son capaces de sustituir o garantizar la misma efectividad que un simulacro, pero dentro del compromiso entre servicio y coste, proporcionan una seguridad aceptable.

Las acciones que deberán realizarse para garantizar un buen mantenimiento del plan son las siguientes

- Realizar llamadas de teléfono a todos los contactos que aparecen en el plan. De esta forma se puede garantizar que las personas que asumían las responsabilidades siguen siendo las mismas y que su teléfono no ha cambiado. En el caso de que hayan cambiado, será el responsable del plan quien se encargue de identificar a la nueva persona, o el nuevo teléfono si es este el que ha cambiado. Sería conveniente realizarlo con una periodicidad mensual
- Verificar la replicación de datos entre el CPD principal y el de respaldo. Para el éxito del plan, es fundamental que los datos sean consistentes y estén replicados de la BD principal a la de respaldo, y que los datos están actualizados. Para comprobarlo simplemente es comparar los logs de transacciones de ambas BBDD, y ver que las operaciones que se realizan son las mismas, teniendo en cuenta el retardo de tiempo. Se recomienda realizarlo semanalmente, dado que es una tarea sencilla y poco costosa en tiempo.
- Comprobar que el backup de las aplicaciones y los datos se realiza correctamente. La mejor forma de verificarlo es restaurar los datos en un entorno de pruebas, que podría ser un entorno virtual. En dicho entorno se puede reproducir el entorno de

producción de una forma sencilla y económica, y se puede comprobar que no hay problemas en la restauración. Para el caso de los datos, refiriéndonos a ficheros tal cual, es muy sencillo comprobarlo. En el caso de una base de datos o de alguna aplicación como alguna de las telealarmas supone una mayor carga de trabajo, pero es importante garantizar que se dispone de un backup operativo. Se recomienda realizarlo con una frecuencia bimensual.

- Reuniones mensuales entre el responsable del departamento de IT y el responsable del plan. En ella se contará con la presencia tanto del responsable del CAU, como de los ingenieros que participan en el plan. El objetivo de dicha reunión debe ser confirmar con el departamento de IT que se dispone de toda la información relativa a cambios que hayan podido darse en la infraestructura y que puedan afectar al plan. Asimismo, desde el departamento de IT se facilitará toda la información relativa a nuevos proyectos en desarrollo y su impacto en el plan.

Con estas acciones, podemos garantizar que se realiza un correcto mantenimiento del plan, y que disponemos de suficiente información al respecto para introducir los cambios que sean necesarios y que la efectividad del plan sea la adecuada. La obsolescencia del plan podría provocar el mismo efecto que no disponer de un plan de contingencia.

5.1.2.4.3 Revisión del plan

Una vez completado el plan de mantenimiento y la fase de pruebas, estamos ya en condiciones de realizar una revisión completa del plan. Se trata de revisarlo en su totalidad, teniendo en cuenta todas las conclusiones que hemos ido obteniendo durante todas las fases del proyecto ya completadas.

Con respecto a la fase de comprensión de la organización, se ha realizado un análisis de impacto que ha permitido ver los procesos afectados por el plan y tener la certeza de incluirlos todos en el alcance. También esta fase ha incluido la identificación y análisis de riesgos, con el objetivo de reducir su impacto sobre el negocio.

En cuanto a la estrategia de continuidad de negocio, se han contemplado los tres factores más relevantes: alta disponibilidad, recuperación ante desastres y protección de datos.

En lo concerniente al desarrollo e implantación del plan se han definido los diferentes procedimientos de aviso y actuación, las personas y/o equipos implicados en el plan, así como las funciones y responsabilidades de cada una de ellas, junto con las dependencias que los relacionan. Y por último, se han generado los procedimientos de actuación ante desastres, así como la estrategia de vuelta a la normalidad.

En lo relativo a pruebas y mantenimiento del plan, se ha elaborado una batería de pruebas que engloba la mayoría de las casuísticas de incidencias que se puedan producir y se han ejecutado con éxito. De estas pruebas, se han obtenido datos que pueden mejorar el plan, como por ejemplo tratar de concienciar al CAU y a los usuarios que abran incidencias que cuanto más detallada sea la descripción, más rápida será su resolución. Además, se ha elaborado un procedimiento de mantenimiento del plan, que permitirá mantenerlo siempre actualizado.

5.1.2.5 Introducción del plan en la organización.

Una vez definido el plan en su totalidad, incluida la revisión del mismo, el siguiente paso es su implantación en la organización. Para ello, es fundamental disponer del apoyo de la dirección, tanto financiero, como desde el punto de vista organizativo. Es necesario que desde todas las divisiones, departamentos o áreas de la empresa, se valore la utilidad del plan. En el caso que nos ocupa, y puesto que el plan de contingencia se centra en un departamento, es más sencilla esta concienciación y apoyo.

- Formación del personal

Para que el plan de contingencia funcione según lo esperado, es necesario un plan de formación del personal que interviene en el mismo.
Las acciones formativas que deberán desarrollarse serán las siguientes:

- Operadores del CC24h

Los operadores del CC24h deberán recibir formación básicamente en cuanto a descripción de incidencias para agilizar su resolución. Por ello, se preparará para ellos un taller sobre cómo detectar los detalles importantes desde el punto de vista de IT en cuanto a las incidencias. En dicho taller recibirán formación sobre cómo proporcionar la información con la mayor precisión posible para que el CAU pueda asignarla a la persona o equipo adecuado.

- Responsable del plan

El responsable del plan deberá recibir formación específica sobre la gestión de equipos de trabajo y sobre habilidades comunicativas. Su labor principal es la de coordinar los diferentes equipos, por lo que su formación en dicha gestión es fundamental.

- Responsable del CC24h

Al igual que el responsable del plan, las acciones formativas de este perfil se concentrarán en el desarrollo de las capacidades comunicativas, de gestión de equipos y de gestión de emergencias.

- Equipo técnico

El equipo técnico que engloba a los diferentes ingenieros de cada una de las áreas recibirá dos tipos de formaciones básicas: técnica centrada en su área específica y de gestión de emergencias.

- Concienciación del personal afectado.

Con respecto al personal afectado por el plan, tanto del departamento CC24h como del departamento de IT, es necesario ejercer una concienciación para que tengan en mente la importancia del plan para el negocio de la empresa. Por ello, se organizará un workshop de 3 horas divido en varios turnos en el que se insistirá en la importancia del plan, y solicitarles su máxima colaboración.

- Concienciación de la dirección

Para concienciar a los directivos de la empresa, se prepara una presentación con las cifras económicas de viabilidad del plan y con un informe de la tasa de retorno de la inversión. Además se hará hincapié en la importancia que tiene para la imagen de empresa la continuidad del negocio y el cumplimiento de la normativa.

- Inversiones en infraestructura

Además de las labores de formación y concienciación, se requerirá de una inversión en la infraestructura, para acometer las compras necesarias del CPD secundario.

Una vez realizadas todas estas tareas formativas y de concienciación, podemos considerar que el plan está listo para proceder a su implantación en la organización y se puede continuar con las tareas del mismo.

5.2 Aportaciones al estado de la cuestión.

Durante la realización del proyecto se alcanzó el objetivo de la creación de plan de contingencia que permitirá garantizar el servicio del CC24h ante cualquier incidencia que pueda surgir. Se creó un procedimiento completo que es capaz de responder ante cualquier incidencia que se produzca, sea parcial o total en el sistema.

El plan generado incluye la implementación y mantenimiento de un centro de respaldo desde el que proporcionar el servicio en caso de desastre, utilizando la estrategia de desarrollarlo con recursos propios en lugar de por medio de un outsourcing.

El CC24h es un departamento clave en la empresa tal y como se ha detallado en anteriores capítulos. Ser capaces de garantizar su funcionamiento en cualquier circunstancia, ante cualquier tipo de incidente, es fundamental para la empresa. Tanto desde el punto de vista económico, como desde el punto de vista de imagen de la empresa, es realmente relevante mantener el servicio.

Adicionalmente, se consiguió documentar toda la actividad del departamento, los diferentes procesos que se llevan a cabo en el funcionamiento diario.

5.3 Procedimiento implementando

Se estableció un procedimiento global que permite acometer y solucionar a la mayor brevedad posible cualquier incidencia que pudiera suceder en el ámbito de departamento CC24h, y que afecte a cualquiera de las herramientas utilizadas en los procesos de trabajo.

El procedimiento comienza con la detección de un fallo en el funcionamiento de alguno de los subsistemas o bien en el sistema completo por parte de algún usuario del mismo, o bien por parte de las herramientas de monitorización del departamento de IT. El primer paso consiste en abrir incidencia en el Centro de Atención a Usuarios (CAU), bien por teléfono, bien por correo electrónico.

Cuando el CAU abre la incidencia y se percata de que afecta al CC24h, se pone en contacto con el responsable del plan, facilitándole toda la información disponible con respecto al incidente. El responsable realiza una evaluación de la misma y decide si se trata de una avería parcial o total del sistema.

En caso de que se trate de una avería parcial, el responsable identifica el subsistema o subsistemas a los que afecta, y contacta con el responsable o responsables de soporte correspondientes. Ellos, realizan una evaluación técnica, y en caso de poder resolverla por sus propios medios, lo hacen. En caso de que sea necesaria intervención de algún soporte de terceros, contactan con ellos y se aseguran de que la incidencia quede resuelta a la mayor brevedad posible.

En el caso de avería total del sistema, el responsable del plan contacta con todos los responsables de todas las áreas, informándoles de lo sucedido. En el caso concreto del responsable del CC24h, se le informa de que los operadores deben trasladarse al CPD de respaldo. En paralelo cada uno de los responsables de área realiza las operaciones que tiene asignadas y confirma al responsable del plan que el servicio se puede seguir operando desde el CPD secundario.

Una vez recibida la confirmación, el responsable del plan informa al CAU, el cual procede a informar al usuario que abrió la incidencia de que ha sido resuelta, y mantener los tiempos del procedimiento habitual de gestión de incidencias.

5.4 Plan de mejora continua

Además del plan implementado, el proyecto incluye la mejora continua del mismo. Para dicho propósito, se establece una reunión bimensual del responsable del plan con los responsables de cada una de las áreas, incluyendo al responsable del CC24h. El objetivo de dicha reunión es el de identificar posibles deficiencias del plan y discutir de forma interna como mejorarlas, así como concluir las medidas a tomar y su implementación dentro del plan.

La reunión se fija cada dos meses, aunque susceptible de adelantarse en el caso de que alguno de los implicados lo considere necesario. Se considera dos meses un tiempo adecuado para no saturar de reuniones, pero al mismo tiempo poder mantener al día las necesidades o cambios que puedan ser necesarios en el plan para su mejora.

Adicionalmente se plantea la posibilidad de que asista a la reunión un operador del CC24h, que pueda dar una visión más cercana al día a día del funcionamiento del departamento.

El orden del día de dicha reunión será:
1. Revisión general del servicio
2. Deficiencias encontradas
3. Cambios propuestos
4. Modificaciones en el plan (si fueran necesarias)
5. Gestión de cambios

El responsable del plan será el encargado de convocar dichas reuniones y de reservar sala para el desarrollo de la misma. También tendrá la responsabilidad de elaborar el acta, y gestionar que los cambios de mejora propuestos se puedan implementar.

El plan de mejora continua junto con el plan de mantenimiento se consideran fundamentales, por lo que se realizará una reunión de concienciación con la dirección para explicar su importancia y conseguir el apoyo necesario. Es muy importante implicar a la empresa en su conjunto, incluyendo la dirección.

6 Resultados y conclusiones

Como resultado del proyecto disponemos de un plan de contingencia para el Centro de Control 24h, basado en un análisis pormenorizado del funcionamiento de dicho departamento, así como en los requisitos funcionales y restricciones del mismo. El procedimiento definido, que incluye cambios en la infraestructura junto con los pasos a seguir para reestablecer el servicio en caso de contingencia total o parcial, cuenta con una serie de procesos y personas implicadas, que permite el restablecimiento de estos servicios, tan críticos para la compañía.

Algunos de los objetivos incluidos dentro del objetivo global no pudieron completarse con éxito. Por ejemplo no se consiguió realizar un simulacro en el caso más desfavorable (caída del sistema completo en un fin de semana por la noche), porque no fue autorizado por la dirección. Se asumió por parte de los responsables que los simulacros no se realizaron en el caso peor, por lo que si sucede una contingencia de ese tipo, no se garantiza que los tiempos de respuesta sean los conseguidos en los simulacros.

Otros objetivos parciales, pero de relevancia dentro del proyecto, si fueron alcanzados, como por ejemplo la realización de entrevistas al personal del CC24h para obtener información sobre los procesos, o la realización de un simulacro un día laborable durante el horario laboral.

En conclusión podemos afirmar que se alcanzó el objetivo inicialmente propuesto en la planificación del proyecto, que se cubrieron buena parte de los objetivos parciales, y que se dispone de un plan de contingencia que permite mantener operativo el CC24h tal y como se había planteado.

7 Desarrollos posteriores

Como principal desarrollo posterior se propone la realización de una aplicación que pueda centralizar las contingencias que pueda ocurrir en los servicios del CC24H.

Otro desarrollo posterior que ha quedado fuera del ámbito de este proyecto, se podría incluir la aplicación desarrollada dentro de CAT y que al seleccionarse alguna de las contingencias, la propia aplicación aprovechando el módulo de envío de mensajes avisará mediante SMS a las personas afectadas.

También se podría implementar una herramienta de gestión del servicio, que actuara sobre él de forma reactiva, avisando a los administradores de averías desde el mismo momento en que se produzcan, incluso resolviendo algunas sencillas o poniéndose en contacto con el soporte técnico del proveedor por email. Por ejemplo, ante el caso de una avería en la centralita telefónica o en la línea de acceso a Internet, que pudiera enviar

un email al operador de comunicaciones informándole, abriendo una incidencia y dando el contacto de la persona o departamento al que tendría que avisar una vez resuelta.

También podría modificarse el plan para que el CPD de respaldo fuera en modo outsourcing. Habría que preparar un RFQ (Request for quotation) para que los proveedores lo completaran con su oferta. Dicha oferta debería incluir no solo precios, sino detalles en profundidad de los servicios que incluiría y los SLA's de los mismos. Es importante definir con el máximo detalle posible, puesto que las especificaciones pueden considerarse obligaciones legales si hubiera algún problema con el proveedor. Sin duda el outsourcing no es una buena opción para un servicio tan crítico como este, pero habría que revisar los costes y compararlos, porque para un servicio con tan baja tasa de utilización puede ser rentable. Las posibles ventajas de este escenario serían por un lado la experiencia técnica del proveedor y el ahorro de costes. Aunque en ambos casos, había que verificarlo previamente y no darlo por supuesto.

Otro posible desarrollo, sencillo de llevar a cabo, sería la implementación de la aplicación en inglés. Dado que se trata de una multinacional del sector de la elevación, sería conveniente disponer de una versión en inglés, para poder utilizarla en el resto de países. Para ello, toda la lógica y desarrollos llevado a cabo de la aplicación serían perfectamente utilizables, simplemente habría que modificar la parte del interfaz, y el manual de usuario.

También sería posible el desarrollo de cara al futuro de una base datos de conocimiento sobre incidencias sucedidas en los sistemas del CC24h. De esta forma, ante cualquier incidencia, los ingenieros podrían consultar en primer lugar esta base de conocimiento y tratar de encontrar la solución óptima a cualquier problema que surgiera en cualquier servicio.

Otra propuesta de desarrollo futuro sería la de sustituir la telefonía tradicional por telefonía IP. De esta forma se conseguiría más independencia del operador, puesto que se podrían realizar los cambios de configuración directamente por parte de personal técnico de la empresa, sin depender de terceros.

8 Bibliografía

Para la realización de este proyecto se han consultado las siguientes fuentes de información:

Titulo	Autor
UNE-EN ISO 22301:2015 Web de Aenor http://www.aenor.es	Aenor
Complejidad tecnológica, Universidad de Antioquía 2012	Alberto Muñoz Rave
Business Continuity: Best Practices. – Editorial: Rothstein Associates; 2000 edition (June 10, 2000)	Andrew Hiles
The Definitive Handbook of Business Continuity Management, 2011	Andrew Hiles
The evolution of business continuity management: A historical review of practices and drivers. October 2010	Brahim Herbane
A Management Guide to Implementing Global Good Practice in Business Continuity Management, 2010	Business continuity institute
Business Continuity Management Policy and Framework, March 2010, http://www.sheffield.ac.uk/polopoly_fs/1.1065!/file/BusinessContinuityPolicy.pdf	Business Continuity Steering Group, The university of Sheffield
8 steps for planning your emergency and disaster plan, 2009	Business Development Bank of Canada
La importancia de proteger los sistemas informáticos críticos, Asociación para el progreso de la dirección, http://www.apd.es	CA Technologies, APD
Planes de contingencia, 2006, www.belt.es	César Mayoral
Informe sobre el funcionamiento del mercado de ascensores en España, Comisión Nacional de la competencia, septiembre 2011.	CNMC
Business continuity and disaster recovery planning: The basics, CSO, May 2015	Derek Slater
Documentación técnica de Dielro http://www.dielro.com	Dielro S.L.
Benefits of Business Continuity Planning, 2011	Disaster Recovery Org
Business Continuity Management: A Crisis Management Approach, 2010	Elliott D, Swartz E and Herbane B
Las TI como servicio, el desafio de la gestión.IDC	Fernando Maldonado
Políticas de continuidad del servicio: Planes de Contingencia - Comisión nacional del mercado de valores	Francisco Javier Nozal Millán
A Guide to Business Continuity Planning, Public Safety Canada, 2013	Government of Canada
Business Continuity Planning Checklist, 2013	Indiana University, USA

https://protect.iu.edu/emergency/bcp/checklist	
Guía práctica de gestión de requisitos, Inteco,	Inteco
Plan de Contingencia informático, Mayo 2012	IVAI, Instituto Veracruzano de acceso a la información
A Guide to Business Continuity Planning– Editorial: John Wiley & Sons; 1st edition (May 2001)	James C. Barnes
MIT Business continuity plan, 1999	Jerry Isaacson, MIT
How to Create an Effective Business Continuity Plan, November 2014, CIO	Kim Lindros and Ed Tittel
Captura de los requisitos. De la visión a los requisitos. 2008	Lic. Espinoza Robles
Estudio sobre el sector de Ascensores, MCA-UGT y Ministerio de Industria, 2012	MCA-UGT
Business Continuity Management Policy, 2011	NSW Government
Business Continuity Policy Statement, January 2013, https://www.brookes.ac.uk/services/hr/business_continuity/policy.pdf	Oxford Brookes university
Análisis y gestión de requisitos, Universidad Rey Juan Carlos, 2009	Paloma Cáceres
Sample business continuity plan template for SMBs, 2012	Paul Kirvan
Planes de continuidad del negocio, http://www.acis.org.co/fileadmin/Conferencias/ConferenciaBCP.pdf	Ramiro Merchan Patarroyo y Plinio Esteban Palomino
Best Practices for Business Continuity Management Governance Gartner Consulting, http://www.gartner.com	Roberta J. Witty , Louis Boyle
El Análisis de Criticidad, una Metodología para mejorar la Confiabilidad Operacional	Rosendo Huerta Mendoza
Introduction to Business Continuity Planning, 2005	SANS Institute
Plan estratégico de TI, Caprecom (Caja de previsión social de comunicaciones, Bogotá)., Junio 2014	Saúl José Pérez
IT business continuity, disaster recovery strategy guide for CIOs, 2013	SearchCIO.com
Business continuity planning, January 2015	State of Queensland
State of datacenter 2012, Symantec report, 2012 may, http://www.symantec.com	Symantec INC.
The concept and context of business continuity, 2010	The London School of economics and political science
Business Continuity Management Policy, March 2010	Victoria Unversity of Wellington
How to create a business continuity plan, 2013 September, http://www.wikihow.com/Create-a-Business-Continuity-Plan	wikiHow

9 Anexos.

9.1 Anexo A: Entrevistas al personal del CC24h

En este anexo se recogen las entrevistas realizadas al personal del departamento CC24H. En concreto se entrevistó a la responsable del departamento M.G., a uno de los ingenieros de telecomunicaciones A.J. y a una de las operadoras, A.L.

Transcripción de la entrevista a M.G. responsable del departamento CC24h.

- E.- Bueno, en primer lugar me gustaría saber qué opinas de la necesidad del plan de contingencia para los servicios que se prestan en tu departamento.
- MG.- Pues llevamos ya tiempo demandando algo así. En los últimos 5 años el mercado de la postventa en elevación ha cambiado mucho. Una vez que la construcción cae y nuestro negocio de obra nueva pasa a ser secundario, todas las empresas de elevación han centrado su negocio en la postventa. Nosotros nos ponemos manos a la obra para conseguir el mayor parque de mantenimiento posible de aparatos, y la competencia también. Y claro, esto lleva a que la orientación de la empresa al cliente tenga que ser total. Si la satisfacción y la percepción de calidad del servicio antes era importante, ahora es vital. Ello ha llevado a que se firmen contratos cada vez con mejores condiciones para el cliente y a un menor coste. Y claro, nosotros no podemos permitirnos otra cosa que no sea hacer las cosas lo mejor posible y con los costes más bajos.
  Dentro de esa política de buscar la excelencia y la satisfacción del cliente, es donde encuadramos este plan de contingencia para mi departamento, que como sabes, es uno de los que más relación tiene con el cliente. Para nosotros es fundamental atender al cliente 24 horas al día, evidentemente solo a aquellos que lo demandan. Y para ello este plan es fundamental, porque nos va a garantizar que podamos dar ese servicio.

- E.- De acuerdo. ¿Qué importancia estratégica tiene el servicio 24 horas?
- MG.- Pues mucha, y te lo ilustro con un ejemplo. Hay una importante cadena de supermercados que es nuestro cliente. Y tenemos firmados contratos con ellos en los que nos comprometemos a reparar cualquier aparato en menos de 4 horas. Por tanto, si mi departamento en cualquier momento no tuviera acceso a los sistemas para tramitar una incidencia y llegáramos tarde, tendríamos penalizaciones económicas. Aunque eso no es lo importante, lo importante sería el riesgo de perder a ese cliente. En este caso concreto es uno de nuestros clientes VIP, que representa un porcentaje muy importante de nuestro parque de mantenimiento, uno de los grandes de nuestra cartera de clientes… así

que imagina lo que podría suponer no tener este plan de contingencias y no poder atender los compromisos.

- E.- ¿Qué esperas de este plan?
- MG.- Pues espero varias cosas. La primera es que no nos suponga trastorno en el día a día. Entendemos que habrá que hacer alguna prueba, incluso algún simulacro. Pero queremos tener la garantía de que mi gente podrá sacar adelante el trabajo en todo momento.
  Por otro lado, espero que me dé seguridad. Que una vez puesto en marcha, yo pueda irme tranquila de vacaciones o el fin de semana, sabiendo que en caso de cualquier incidencia, parcial o completa, el sistema estará operativo en los tiempos que veamos cómo razonables.

- E.- Ahí quería llegar. ¿Cuáles son más o menos los tiempos razonables para cada servicio?
- MG.- Pues mira, para cada servicio en concreto, háblalo con uno de los ingenieros de telecomunicaciones. Pero ya te adelanto que nos es imposible trabajar más de 4 horas en fin de semana sin el CAT y sin la mensajería móvil. Entre semana, en horario laborable, tenemos más margen porque cada delegación provincial es capaz de gestionar las incidencias de su provincia. Pero el fin de semana y los festivos, los festivos nacionales sobre todo, todas las llamadas se centralizan aquí. Y eso significa un volumen de trabajo tremendo, que no puede gestionarse sin las aplicaciones.

- E.- Muy bien, y que me dices de las comunicaciones: telefonía, fax, correo electrónico
- MG.- La telefonía es clave. Cuando hay un rescate de una persona atrapada en un aparato, siempre nos llega la incidencia por teléfono. Es decir, siempre tenemos que tener teléfono para atender las llamadas. Y sobre todo en fin de semana es imprescindible tener una centralita digital que nos permita hacer cambios sobre la marcha, activar o eliminar extensiones, tener siempre flexibilidad.
  El fax y el correo electrónico también son importantes, pero podemos prescindir de ellos algo más de tiempo.

- E.- ¿Y qué me dices del resto de servicios, como los datos del departamento?
- MG.- Bueno, también los necesitamos. Tenemos abundante documentación, tanto de procedimientos que seguimos, como procesos del departamento, así como otra información no tan estratégica, pero que es terriblemente práctica, como puede ser el listado de teléfonos de técnicos de reparación, el calendario de trabajo del departamento, o una base de datos que tenemos donde se registran observaciones que los operadores recogen antes de terminar su turno. No es tan importante como tener el CAT o la mensajería móvil, que son imprescindibles y que no podemos pasar sin ellos más de 4 horas. Pero si necesitamos disponer de ellos en un tiempo que no pude ir mucho más allá de 8 o 9 horas.

- E.- Pues no tengo más preguntas. Creo que con esto me queda claro en líneas generales como es el servicio que dais, y cuáles son vuestras necesidades. Ya entró más en detalle con la gente de tu departamento. Muchas gracias.
- MG.- Gracias a ti, y suerte con el proyecto. Si necesitas algo más, ya sabes donde encontrarme.

Transcripción de la entrevista a A.J. ingeniero de telecomunicaciones del departamento CC24h.

- E.- Ya hemos hablado con la responsable del departamento sobre temas generales, nos gustaría concretar un poco más contigo.
- A.J.- Por supuesto, cuéntame que quieres saber

- E.- Pues mira, una de las cosas que tengo que concretar contigo son los tiempos máximos que podéis asumir sin servicio. Quiero decir, cuanto tiempo podéis estar sin CAT, sin mensajería móvil, sin correo electrónico,…
- A.J.- En primer lugar hay que decir que los días laborables y los festivos y fin de semana son muy diferentes para nosotros. En los días laborables, las 100 delegaciones que tenemos están funcionando. Eso significa que cada una atiende su zona de influencia, con lo que no es tan crítico que tengamos operativo el Call Center central. En cambio, en fines de semana y festivos nacionales, desde estas instalaciones se atiende a toda España. Tenemos un parque de mantenimiento en nuestra cartera de clientes de unos 130.000 aparatos, entre ascensores y escaleras mecánicas. Aunque solamente haya un 0,005 % de averías un domingo, tendríamos 650 llamadas, e irían todas al CC24h de la central. En cambio si esto ocurre un lunes no festivo, esas llamadas se repartirían entre las 100 delegaciones, con lo que tendríamos mucho más tiempo de reacción. En festivos y fin de semana vamos a poder contar con muy poco margen si queremos dar un servicio de calidad.

- E.- Bien, si te parece vamos a ver entonces cada uno de los servicios, teniendo en cuenta que no tenemos el mismo margen de tiempo los festivos y fines de semana que los días laborables. Por ejemplo, el CAT y los mensajes a móviles, ¿cuánto tiempo podéis trabajar sin ellos?
- A.J.- En días laborables yo creo que hasta 8 horas sería asumible. En fin de semana, no más de 4 horas. No todos los festivos hay las mismas llamadas, pero en un típico día, dentro de la media, más de 4 horas sin estos dos sistemas, nos saturarían. Ten en cuenta que sin ello, hay que hacer todo manual, recoger los datos en una hoja de Excel o algo así, y luego pasarlo al CAT cuando se recupere el servicio. Con los mensajes a móviles igual, hay que enviarlos a mano. Aunque el proveedor de comunicaciones nos facilite alguna herramienta para no tener que hacerlo en el móvil, tendríamos problemas.

- E.- Y, ¿Cuáles serían los tiempos para los servicios de comunicaciones como el email o el fax?
- A.J.- El fax lo tenemos solucionado en 4 horas por el operador de comunicaciones. Se compromete con nosotros a que en menos de ese

tiempo, puede desviar nuestro número de fax a cualquier teléfono que le digamos, siempre y cuando sea dentro de la misma provincia. Y esto es válido tanto para festivo como para día laborable, su servicio es 24x7.
Con respecto al email, quizá podríamos estar sin este servicio 8 horas en un día laborable, y en ningún caso más de 4 en un festivo o fin de semana. Para nuestro trabajo es muy importante. Hay muchas gestiones con proveedores que las hacemos directamente con el email. Tenemos también un número de teléfono, pero es mucho más cómodo por correo electrónico, porque queda registrado, y porque además tenemos la opción de enviar y recibir documentos adjuntos.

- E.- ¿Y qué me dices del resto de servicios?
- A.J.- Pues nuestros datos que están alojados en el servidor, los datos del departamento, los necesitaríamos en los mismos tiempos que las aplicaciones principales: 8 horas en día laborable como máximo, 4 en festivo. Ten en cuenta que ahí tenemos un montón de documentación del día a día.
Y en los demás servicios tenemos mucho más margen, no son servicios tan críticos. Las telealarmas con tenerlas en 24 horas nos vale. Los aparatos envían la alarma cada 3 días y el proveedor de comunicaciones nos mantiene los mensajes durante 48 horas, aunque no tengamos disponibles los servidores que los almacenan. Da igual que sea festivo que laborable, hasta 24 horas sin telealarma, no sería un problema. Y lo mismo para el servidor de escaleras. Aunque no lo tengamos en un día, podemos funcionar sin mayor problema.
Por último quedaría comentar el servicio de llamadas de emergencia, cuando una persona se queda atrapada y quiere utilizar el propio sistema del ascensor. Podemos prescindir de él durante 8 horas sin problema, porque las llamadas se puede redirigir sin problema al teléfono que queramos.

- E.- Entendido. ¿Utilizáis alguna otra herramienta o aplicación adicional, por ejemplo impresora, escáner o similar?
- A.J.- Tenemos alguna impresora en el departamento, porque a veces hay que imprimir alguna cosa. Pero realmente nosotros no trabajamos con ofertas, ni con pedidos, ni con ningún tipo de documento que haya que enviar en papel. Y lo mismo con el escáner. Dada la complejidad del proyecto en si, no creo que tengáis que tener en cuenta este tipo de dispositivos o servicios que para nosotros no son importantes.

- E.- Una cosa más, ¿Qué tasa de fallos tienen los sistemas específicos que utilizáis vosotros?. Me refiero al CAT, las telealarmas, el envío de mensajes a móviles,…
- A.J.- Pues la verdad es que el porcentaje de disponibilidad de los mismos es alto, solemos estar en el 99,99998% mensualmente. Ten en cuenta que son estratégicos para el negocio. Dar un buen servicio al cliente es fundamental en un mercado tan competitivo como este.

- E.- Bien, bien.. y, ¿estos servicios tan automatizados que ventajas ofrecen en la operativa del día a día?

- A.J.- Por ejemplo, la combinación de CAT para recoger la incidencia de un aparato con servicio de mensajería móvil hacen que el proceso se agilice en un 70% con respecto a cómo lo hacíamos antes. El CAT tiene registrados los números de teléfono de los clientes y el del propio ascensor, de forma que en cuanto la llamada entra en el Call Center, ya está identificado y el operador tiene acceso a todos los datos del mismo, incluido el historial técnico y todos los datos que puede necesitar un técnico para poder ir a repararlo en muy poco tiempo. Con un solo click puede enviar al técnico la información, con lo que en muy poco tiempo, se puede proceder al rescate. Bueno, luego es verdad que el técnico tiene que ir, aparcar, llegar hasta el aparato… pero eso ya es otro tema.
  Lo mismo pasa con las telealarmas. Este sistema nos avisa de las averías de los aparatos, nos avisa de cuando hay que hacer las revisiones, incluso en algunos casos es capaz de avisarnos de cuando una pieza aún no ha fallado, pero está próxima a hacerlo, en función de ciertos parámetros. Y nos envía también estadísticas de uso del ascensor, lo cual nos es muy útil, porque nos permite saber cómo se está usando ese ascensor, cuando tiempo está detenido, en que momento del día es cuando menos se usa….. Con todos estos datos, nosotros analizamos cual es la mejor forma de realizar ese mantenimiento del ascensor, y esas reparaciones. Incluso si vemos que algo va a fallar, podemos ir a cambiarlo antes, evitando una avería mayor. La ingeniería de postventa es fundamental para nosotros, en nuestro reto de dar el mejor servicio, y los datos que nos facilitan estas aplicaciones son clave.

- E.- También quería comentar contigo el tema de la telefonía, la gestión de llamadas, las prioridades de las mismas, los puestos de operador.. Como lo hacéis
- A.J.- Es fundamental tener una centralita que nos permita gestionar las llamadas y asignarlas de forma dinámica a los operadores. También es importante que tengamos flexibilidad a la hora de añadir nuevas extensiones, o eliminarlas, en función de si tenemos más o menos operadores trabajando en ese momento. La centralita tiene que ser capaz de pasar la llamada a los operadores

- E.- ¿Necesitáis disponer de acceso a Internet para alguna de las operaciones que realizais habitualmente?
- A.J.- Pues sí. En concreto algunas de las operaciones que requerimos del operador de comunicaciones pueden hacerse por Internet de una forma bastante ágil. Si no tuviéramos Internet podríamos hacerlo por teléfono, pero es mucho más lento. A fin de cuentas lo que hace la persona que nos coge la incidencia o el cambio de configuración es introducir los datos en esa aplicación, si lo hacemos nosotros, ganamos tiempo.

- E.- De acuerdo, pues muchas gracias.
- A.J.- De nada, para eso estamos.

Transcripción de la entrevista a A.L. operadora del departamento CC24h

- E.- Bueno, quería hacerte algunas preguntas en relación con el plan de contingencia que estamos elaborando. ¿Cómo es el proceso de recogida de una incidencia?
- A.L.- Pues nada más que el cliente realiza la llamada, bien desde su teléfono bien desde el ascensor, se recibe aquí. Hay un sistema que asigna las llamadas a cada operadora, en función de las que estén libres, del número de llamadas atendidas. Además en el display podemos ver las que hay en espera, para tratar de agilizar las que tenemos en curso. En cuanto la llamada te entra, en el display del teléfono aparece el teléfono desde el que te llaman, y lo que hacemos es introducirlo en el CAT. Si es uno de los teléfonos que tenemos registrado para ese ascensor, porque sea el cliente quien llama o una llamada con la línea del operador, automáticamente nos aparecen todos los datos del aparato.
  Si no, hay que pedir al cliente algunos datos, para poder identificar el aparato. En principio con una pegatina que tenemos colocada dentro del ascensor, podemos identificarlo con un código.

- E.- De acuerdo, y una vez identificado el aparato elevador, ¿cuál es el siguiente paso?
- A.L.- Lo siguiente es tratar de identificar qué tipo de avería es. Siempre preguntamos si hay alguien atrapado, y si es así, rápidamente desde el mismo CAT, enviamos un mensaje al técnico correspondiente, utilizando la aplicación de mensajes a móviles. Es importante que el rescate se realice en menos de una hora desde que recibimos la llamada. Lo normal es que el técnico puede realizar el rescate en menos de media hora, menos aún si es en ciudades pequeñas. En el caso de que no sea un rescate, revisamos de que cliente se trata, por si fuera uno VIP. En ese caso, también enviamos al técnico urgente, porque depende del cliente, tenemos contratos que nos obligan a solucionar la avería en menos de 4 horas. Y en el caso de que sea un cliente estándar, simplemente enviamos el mensaje al técnico de la zona para que lo ponga en su cola de tareas y lo atienda cuando vaya terminando las anteriores.

- E.- ¿El trabajo es igual en día laborable que en festivo?
- A.L.- Que va, es totalmente diferente. En laborable solo atendemos la comunidad autónoma de Madrid. En fin de semana todo el país, porque las delegaciones no abren, y todas las llamadas se desvían aquí. Además tenemos a veces dificultades para dar los tiempos que vamos a tardar en resolver una avería o en atender un rescate, porque no conocemos las ciudades y no sabemos cuánto podría tardar el técnico. En Madrid es distinto porque conocemos la ciudad, y podemos dar tiempos más o menos aproximados. Los clientes siempre quieren saber cuanto van a tardar en rescatarlos, lo cual me parece normal. A nadie le gusta estar sin ascensor o estar atrapado en un ascensor.
  Y por otro lado está la diferencia en volumen de llamadas. En día laborable tenemos un volumen de trabajo que atendemos entre 4 y 6

personas sin problema. En fin de semana a veces estamos hasta 12, y apenas tenemos tiempo de hacer otra cosa que no sea atender el teléfono.

- E.- ¿Qué más tareas realizais además de atender el teléfono?
- A.L.- Bueno, pues colaboramos con los ingenieros en la gestión de las telealarmas. Les ayudamos a revisar el parque, para comprobar que todos los aparatos están funcionando correctamente. Cuando se detecta alguna incidencia o alguna labor de mantenimiento que no pueda esperar en algún equipo, contactamos con técnico para pasarle el parte de trabajo.

- E.- ¿Tenéis muchos datos departamentales?
- A.L.- Bueno, yo creo que no es un gran volumen de datos, pero tenemos cosas que son importantes y que necesitamos para el día a día. Por ejemplo tenemos un fichero con los turnos que es muy dinámico porque como trabajamos tantos operadores, hay muchos cambios. Es una hoja de Excel, pero es importante para nosotros. Luego tenemos también formularios estándar para el envío de fax, correo electrónico,… que nos facilitan mucho el trabajo y nos hacen ganar mucho tiempo. Son para enviar información a clientes, a algún organismo oficial que lo requiera,… o por si tenemos que enviarle algún manual de algún aparato a algún técnico.

9.2 Anexo B: Norma EN 81-28

Norma	**UNE-EN 81-28:2004**
Título español	**Reglas de seguridad para la construcción e instalación de ascensores. Ascensores para el transporte de pasajeros y cargas. Parte 28: Alarmas a distancia en ascensores de pasajeros y pasajeros y cargas.**
Título inglés	Safety rules for the construction and installation of lifts - Lifts for the transport of persons and goods - Part 28: Remote alarm on passenger and goods passenger lifts
Título francés	Règles de sécurité pour la construction et l'installation des ascenseurs - Elévateurs pour le transport de personnes et d'objets - Partie 28: Téléalarme pour ascenseurs et ascenseurs de charge
Fecha Edición	2004-03-12
ICS	13.320 / Sistemas de alarma y de alerta
	91.140.90 / Ascensores. Escaleras mecánicas
Comité	AEN/CTN 58 - MAQUINARIA DE ELEVACIÓN Y TRANSPORTE
Equivalencias Internacionales	EN 81-28:2003 - Idéntico

ÍNDICE

Página

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma se aplica a los sistemas de alarma para todos los tipos de ascensores de pasajeros y de pasajeros y cargas, en particular a aquellos cubiertos por la serie de Normas EN 81.

Esta norma también se refiere a la información mínima a dar al propietario de la instalación respecto al servicio de mantenimiento y rescate.

Esta norma trata el siguiente peligro significativo relativo a los ascensores cuando son usados como se supone y en las condiciones previstas por el instalador/fabricante:

Atrapamiento de usuarios debido al funcionamiento inadecuado del ascensor.

Esta norma no es aplicable a los sistemas de alarma previstos para utilizarse para pedir ayuda en otros casos, por ejemplo, ataques al corazón, búsqueda de información.

Esta norma es aplicable a los sistemas de alarma utilizados para ascensores fabricados e instalados después de la fecha de publicación por el CEN de la misma. Sin embargo, puede ser considerada en la aplicación a ascensores existentes.

La Norma EN 81-70 expresa requisitos adicionales para personas con discapacidades.

Esta norma anula y sustituye a las Normas EN 81-1:1998 y EN 81-2:1998 en lo que respecta a alarma a distancia (véase el apartado 14.2.3).

2 NORMAS PARA CONSULTA

Esta norma europea incorpora disposiciones de otras publicaciones por su referencia, con o sin fecha. Estas referencias normativas se citan en los lugares apropiados del texto de la norma y se relacionan a continuación. Para las referencias con fecha, no son aplicables las revisiones o modificaciones posteriores de ninguna de las publicaciones. Para las referencias sin fecha, se aplica la edición en vigor del documento normativo al que se haga referencia (incluyendo modificaciones).

EN 81-1:1998 – *Reglas de seguridad para la construcción e instalación de ascensores. Parte 1: Ascensores eléctricos*.

EN 81-2:1998 – *Reglas de seguridad para la construcción e instalación de ascensores. Parte 2: Ascensores hidráulicos*.

EN 81-70:2003 – *Reglas de seguridad para la construcción y la instalación de ascensores. Aplicaciones particulares para los ascensores de pasajeros y de pasajeros y cargas. Parte 70: Accesibilidad a los ascensores de personas, incluyendo personas con discapacidad*.

EN 292-1 – *Seguridad de las máquinas. Conceptos básicos, principios generales para el diseño. Parte 1: Terminología básica. Metodología.*

EN 292-2 – *Seguridad de las máquinas. Conceptos básicos, principios generales de diseño. Parte 2: Principios y especificaciones técnicas*.

EN 1070:1998 – *Seguridad de las máquinas. Terminología*.

EN 13015:2001 – *Mantenimiento de ascensores y escaleras mecánicas. Reglas para instrucciones de mantenimiento*.

9.3 Anexo C: Cálculos viabilidad económica

Los cálculos realizados para el estudio de la viabilidad económica se han realizado solicitando presupuestos a los habituales proveedores. Los resultados son los que se pueden ver en la siguiente tabla:

Concepto	Importe unitario	Total	Coste anual
Servidores	7322,57	14645.15	4881,71
Fax	50	50	10
Centralita	5765,22	5765,22	5765,22
Líneas telefónicas	2330,12	2330,12	2330,12
Línea fax	119,76	119,76	119,76
MPLS conexión CPD principal	4490,16	4490,16	4490,16
PC's operadores	1000	4000	1000
Acceso Internet	2327,19	2327,19	2327,19
Licencia Windows Server 2012	490,83	981,66	981,66
Licencia SQL Server 2012	1994,31	1994,31	1994,31
Licencia Exchange server	393,59	393,59	393,59
CALs Exchange server	75,9	1518	1518

TOTAL: 25.811'73

Los precios del software son anuales en concepto de explotación del producto e incluyen soporte técnico online y actualizaciones gratuitas.

En el caso de Windows Server 2012 standard el licenciamiento se realiza por procesador, facturándose como mínimo dos procesadores por cada máquina. En este caso ambas máquinas tiene dos procesadores de 6 cores, pero solamente es necesario licenciar por procesador.

En la licencia de SQL sucede lo mismo, se paga la licencia por procesador, y de dos en dos unidades. En este caso como la máquina que tendrá instalado SQL tiene dos procesadores, solo tendremos que abonar una licencia.

Para el licenciamiento de Exchange server, y como solo van a ser 20 usuarios como máximo, se ha elegido la licencia de solo servidor, teniéndose que adquirirse individualmente licencias para cada uno de los clientes que vayan a acceder. De esta forma el coste es menor, porque las licencias de acceso cuestan solamente 1518€. Sumándole los 393,59 del servidor, no llega ni con mucho al coste de una licencia de Exchange Server 2012 por procesador.

Las licencias de los equipos de los operadores van incluidas en la compra de los propios equipos. Se trata de licencias OEM que incluyen el sistema operativo, y el software básico de ofimática, Office 2013 professional.

9.4 Anexo D: Datos de contacto y responsables

Con respecto a los datos de contacto de personas implicadas y responsables de cada una de las áreas, se ha elaborado la siguiente tabla:

Persona	Rol	Email	Teléfono
Responsable del plan	Responsable global	Contigenciacc24h@empresa.com	675 900 989
Responsable de telecomunicaciones	Telefonia, móviles, comunicaciones	comunicacionescc24h@empresa.com	678 090 134
Ingeniero de sistemas	Responsable sistemas	sistemascc24h@empresa.com	698 098 112
Ingeniero de aplicaciones	Responsable aplicaciones cc24h	aplicacionescc24h@empresa.com	645 098 120
Ingeniero de hardware	Responsable hardware	Hardwarecc24h@empresa.com	664 098 012
Ingeniero de telecomunicaciones	Responsable red	Networkcc24h@empresa.com	654 090 876
CAU	Atención y gestión de incidencias	cau@empresa.com	902 340 450
Responsable facility Management	Mantenimiento, gestión de accesos	Facility-management@empresa.com	650 430 231

Adicionalmente y para el resto de contactos, se dispone de la siguiente tabla:

Empresa	Soporte	Email	Teléfono
Operador comunicaciones	Comunicaciones	soporteoperador@operador.com	902 330 123
Proveedor hardware	Servidores, portátiles, estaciones de trabajo	soporte@proveedorhardware.com	902 200 100
Proveedor software	Software Sistemas operativos, correo electrónico,…	soporte@proveedorsoftware.com	900 344 130
Dielro	Hardware y software dielro	soporte@dielro.com	902 124 432
Proveedor red	Dispositivos de red, cableado, firewall, proxy	Soporte@proveedorred.com	902 340 564

9.5 Anexo E: Política de continuidad de negocio

Para esta compañía, de ámbito estatal y con más de 90 oficinas, es fundamental contar con un Plan de Continuidad de Negocio que nos permita afrontar con garantías cualquier desastre que se produzca en nuestras instalaciones y que afecte a nuestras operaciones habituales, en concreto en los servicios que ofrece nuestro departamento CC24H. Dichos servicios, son estratégicos para la empresa, especialmente en una coyuntura de crisis y gran competencia en nuestro sector y por eso el alcance de este plan, será de solo dicho departamento, y sus servicios.

Nuestro compromiso con la calidad en el servicio y con la excelencia es tal, que debemos ser capaces de prestarlo en cualesquiera situaciones que se produzcan, incluidos desastres naturales. Es por ello, que pondremos a disposición del Jefe de Proyecto los recursos que sean necesarios, tanto materiales como humanos, incluyendo el Responsable del Plan que estará encargado del mantenimiento del mismo, una vez finalizada la fase de proyecto.

Para garantizar el éxito del mismo, desde el principio definimos adecuadamente las responsabilidades, que recaerán sobre el Jefe de Proyecto mientras se encuentre en desarrollo, y que serán traspasadas posteriormente al Responsable del Plan. Además, involucraremos al Responsable del CC24h para que facilite toda la información requerida para el proyecto.

Además de la importancia estratégica de este departamento que ya hemos señalado, como compañía líder en el mercado, tenemos la obligación de respetar y cumplir la normativa legal. Y no solo la normativa, son también nuestros clientes los que nos demandan un servicio global e ininterrumpido. Y en pos de mantener esos clientes, y del riesgo de perderlos si no cumplimos lo comprometido, son las motivaciones fundamentales que nos llevan a acometer sin demora este proyecto.

Para el desarrollo e implantación de este Plan de Continuidad de Negocio, seguiremos las recomendaciones, buenas prácticas y estándares de calidad de la industria, además de las normativas y regulaciones legales que puedan ser de aplicación.

Firmado:
Antonio Sánchez
Consejero Delegado.

9.6 Anexo F: Presupuesto y planificación del proyecto

La estimación de presupuesto para el proyecto se puede encontrar en las siguientes tablas

Infraestructuras

Recurso	Coste	Observaciones
2 Servidores con sistema de backup *	14645,15€	Se realiza compra del servidor y se realiza amortización del mismo a tres años
Dispositivo de fax	50€	Amortización a 5 años.
Centralita telefónica	5765,22€	El coste es anual, el alquiler a la compañía telefónica. Incluye mantenimiento y modificaciones. Incluye cuatro teléfonos digitales y cuatro analógicos
Líneas telefónicas, primario de voz	2330,12€	Las líneas se incluyen en la centralita y se gestionan desde ella. Este servicio lo da el operador, incluido en el coste de la centralita y una antena para envío de mensajes a móviles.
Línea fax	119,76€	Coste anual de la línea.
Comunicaciones MPLS, 10Mb/10Mb metropolitano	4490,16€	Incluye backup por ADSL 10Mb (10Mb/800Kb). Incluye alquiler de equipos
4 equipos para puesto de operador	4000€	El coste es la compra y se amortizan a 4 años.
Comunicaciones MPLS, acceso a Internet 10Mb (caudal garantizado 4Mb/500kb)	2327,19€	Incluye backup ADSL 10Mb (10Mb/800Kb) y alquiler de equipos.
2 licencias Windows Server 2012 standard	981,66	Precio con software assurance para un año.
1 SQL Server 2012 standard	1994,31	Precio con software assurance para un año.
1 Exchange server 2012 standard + 20 CALs	1911,59	Precio con software assurance para un año.

Total anual infraestructuras al año: 25811,73€

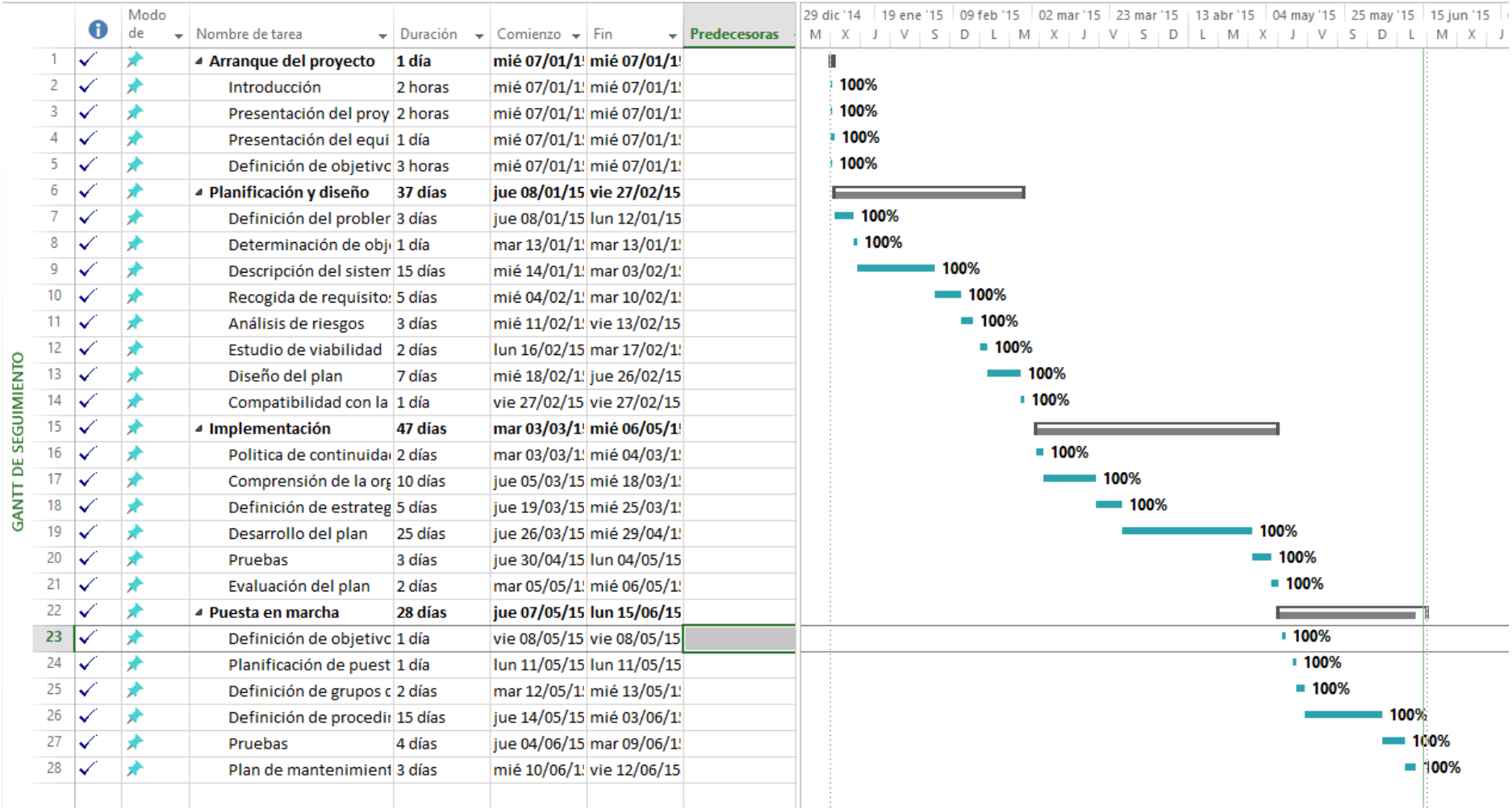
Recursos Humanos

Función	Coste anual	Observaciones
Responsable del plan / Responsable telecomunicaciones	40.000€	Se estima que destinará un 20% de su tiempo al plan.
Ingeniero de sistemas	36.000€	Se estima que destinará un 10% de su tiempo al plan
Ingeniero de aplicaciones	37.000€	Se estima que destinará un 10% de su tiempo al plan
Ingeniero de hardware	34.000€	Se estima que destinará un 10% de su tiempo al plan
CAU	200.000€	Se estima que destinará un 2% de su tiempo al plan.
Responsable CC24H	40.000€	Se estima que destinará un 10% de su tiempo al plan.

Coste total RRHH anual: 26.700€

Presupuesto anual proyecto= 26.700 + 25.811,73 = 52.511.73€

En cuanto a la planificación, se ha realizado según diagrama de Gantt adjunto de la página siguiente.


GANTT DE SEGUIMIENTO
Modo de
Nombre de tarea
Duración
Comienzo
Fin
Predecesoras
1 Arranque del proyecto 1 día mié 07/01/15 mié 07/01/15
2 Introducción 2 horas mié 07/01/15 mié 07/01/15
3 Presentación del proy 2 horas mié 07/01/15 mié 07/01/15
4 Presentación del equi 1 día mié 07/01/15 mié 07/01/15
5 Definición de objetivc 3 horas mié 07/01/15 mié 07/01/15
6 Planificación y diseño 37 días jue 08/01/15 vie 27/02/15
7 Definición del probler 3 días jue 08/01/15 lun 12/01/15
8 Determinación de obj 1 día mar 13/01/15 mar 13/01/15
9 Descripción del sistem 15 días mié 14/01/15 mar 03/02/15
10 Recogida de requisito 5 días mié 04/02/15 mar 10/02/15
11 Análisis de riesgos 3 días mié 11/02/15 vie 13/02/15
12 Estudio de viabilidad 2 días lun 16/02/15 mar 17/02/15
13 Diseño del plan 7 días mié 18/02/15 jue 26/02/15
14 Compatibilidad con la 1 día vie 27/02/15 vie 27/02/15
15 Implementación 47 días mar 03/03/15 mié 06/05/15
16 Politica de continuida 2 días mar 03/03/15 mié 04/03/15
17 Comprensión de la org 10 días jue 05/03/15 mié 18/03/15
18 Definición de estrateg 5 días jue 19/03/15 mié 25/03/15
19 Desarrollo del plan 25 días jue 26/03/15 mié 29/04/15
20 Pruebas 3 días jue 30/04/15 lun 04/05/15
21 Evaluación del plan 2 días mar 05/05/15 mié 06/05/15
22 Puesta en marcha 28 días jue 07/05/15 lun 15/06/15
23 Definición de objetivc 1 día vie 08/05/15 vie 08/05/15
24 Planificación de puest 1 día lun 11/05/15 lun 11/05/15
25 Definición de grupos c 2 días mar 12/05/15 mié 13/05/15
26 Definición de procedi 15 días jue 14/05/15 mié 03/06/15
27 Pruebas 4 días jue 04/06/15 mar 09/06/15
28 Plan de mantenimient 3 días mié 10/06/15 vie 12/06/15
29 dic '14
19 ene '15
09 feb '15
02 mar '15
23 mar '15
13 abr '15
04 may '15
25 may '15
15 jun '15
100%